HOUSE OF COMMONS
CANADA

MAPPING PRIVACY PROTECTION IN THE DIGITAL WORLD: STUDY OF THE PRIVACY IMPLICATIONS OF STREET-LEVEL IMAGING APPLICATIONS

Report of the Standing Committee on Access to Information, Privacy and Ethics

Hon. Shawn Murphy, P.C., MP
Chair

JANUARY 2011

40th PARLIAMENT, 3rd SESSION

Published under the authority of the Speaker of the House of Commons

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site
at the following address: http://www.parl.gc.ca

MAPPING PRIVACY PROTECTION IN THE DIGITAL WORLD: STUDY OF THE PRIVACY IMPLICATIONS OF STREET-LEVEL IMAGING APPLICATIONS

Report of the Standing Committee on Access to Information, Privacy and Ethics

Hon. Shawn Murphy, P.C., MP
Chair

JANUARY 2011

40th PARLIAMENT, 3rd SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Hon. Shawn Murphy

VICE-CHAIRS

Patricia Davidson

Bill Siksay

MEMBERS

Harold Albrecht

Kelly Block

Hon. Wayne Easter

Pierre Poilievre

Hon. Carolyn Bennett

Paul Calandra

Carole Freeman

Ève-Mary Thaï Thi Lac

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Bob Dechert

Jean Dorion

Judy Foote

Greg Rickford

Paul Szabo

Luc Desnoyers

Earl Dreeshen

Russ Hiebert

Michelle Simson

Boris Wrzesnewskyj

CLERK OF THE COMMITTEE

Chad Mariage

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Alysia Davies, Analyst

Élise Hurtubise-Loranger, Analyst

Dara Lithwick, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

ELEVENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*h*)(vi), the Committee has studied the subject of the privacy implications of street-level imaging applications and has agreed to report the following:

TABLE OF CONTENTS

MAPPING PRIVACY PROTECTION IN THE DIGITAL WORLD: THE STUDY OF THE PRIVACY IMPLICATIONS OF STREET-LEVEL IMAGING APPLICATIONS

BACKGROUND

A. The Committee Study

On April 27, 2009, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (hereafter the Committee) passed the following motion:

> That the Committee study the privacy implications of camera surveillance such as "Google's Street View" and "Canpages" and other issues related to video surveillance, and that the committee ask Eric Schmidt, the chairman and CEO of Google, or his Canadian representative, and Olivier Vincent, the chairman and CEO of Canpages, or his representative, to testify before the committee on this subject.

The Committee's study focused on street-level imaging applications, which use various means of photographing the streetscape. Typically, a camera is mounted on a vehicle that is driven up and down the streets of selected cities. The images can then be viewed on the Internet.

The Committee heard testimony from the Managing Director and Head of Google Canada, Jonathan Lister, and President and Chief Executive Officer of Canpages, Olivier Vincent, on June 17, 2009, as well as from the federal Assistant Privacy Commissioner, Elizabeth Denham, on October 22, 2009.

Following the discovery in May 2010 that Google Street View cars had been collecting payload data from unsecured wireless networks as part of its collection of Wi-Fi data, and the Office of the Privacy Commissioner's subsequent investigation into the possible privacy violations of the Wi-Fi data collection, the Committee heard testimony from the Office of the Privacy Commissioner on October 28, 2010 and from Jacob Glick, Canada Policy Counsel for Google, on November 4, 2010. The Committee heard further testimony from Mr. Glick, and Google's new Director of Privacy, Dr. Alma Whitten, via teleconference on November 25, 2010, as well as from François D. Ramsay, Senior Vice-President, General Counsel, Secretary and Responsible for Privacy, and Martin Aubut, Senior Manager, Social Commerce, at Yellow Pages Group (Canpages).

While the focus of the Committee's study has been on the privacy implications of street level imaging, the Google Wi-Fi issue has raised new concerns regarding the need for technology innovators, such as Google, to take measures to adequately incorporate the protection of individuals' privacy in the development of new products.

B. Protection of Personal Information in Canada

The collection, use and disclosure of personal information by commercial organizations in Canada is governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA). However, where a province has introduced its own legislation on this subject that has been deemed "substantially similar" to PIPEDA, organizations covered by the provincial legislation are exempted from the application of the federal Act. Accordingly, in British Columbia, such activity would be governed by the *Personal Information Protection Act*; in Alberta, by the *Personal Information Protection Act*, and in Québec by the *Loi sur la protection des renseignements personnels dans le secteur privé*.[1]

In April 2009, the Privacy Commissioner of Canada, Jennifer Stoddart, sent a letter to the Committee enclosing a fact sheet from her office entitled "Captured on Camera: Street-level imaging technology, the Internet and you" (Appendix A).[2] The fact sheet notes the following privacy concerns raised by the Privacy Commissioner and her provincial counterparts regarding street-level imaging applications:

> Privacy Commissioners have had discussions with several companies to strengthen privacy protections for people whose images are captured. Our position is that all companies that offer such applications must take steps to better safeguard your privacy.
>
> In addition to companies being proactive and creative in their public communications to ensure that Canadians know when their cities—and, therefore, they themselves—may be photographed, we think these companies need to be more privacy sensitive in the areas they choose. They need to be mindful that people entering or leaving sensitive locations, such as shelters or abortion clinics, likely want to remain anonymous for privacy and safety reasons.
>
> They should also use proven and effective blurring technologies for faces and vehicle licence plates, so that people cannot be identified when their images are posted. Where individuals may be identifiable, companies must offer fast and responsive mechanisms to allow the images to be blocked or taken down.
>
> Companies offering these imaging applications must also have a good reason to keep the original, unblurred images in their databanks. If they do retain unblurred images, they must limit how long they keep them and protect them with appropriate security measures.[3]

---

1 In Ontario, there is a slightly anomalous situation—most personal information held by commercial organizations there is regulated under PIPEDA, but the specific category of personal health information is governed by the province's *Personal Health Information Protection Act* instead.

2 Also accessible online at: http://www.priv.gc.ca/fs-fi/02_05_d_39_prov_e.cfm.

3 Ibid.

C. Google Street View

1. The Service

Google Street View is a service created by the web engine company Google Inc. as part of Google Maps. It is intended to replicate the "street view" the user would experience if he or she was walking down the street in any given geographical location around the world. Users can click on a map in the service at: http://Maps.google.ca/streetview, and then take a virtual "walk" through their chosen neighbourhood, which has been reconstructed online using photographic images of the environs.

These photographic images are taken by photographers, who travel around cities and other mapped sites in marked cars with cameras mounted on top. While photographers visited some Canadian cities and began taking photographs in 2007, those images were stockpiled for future use.[4] The official rollout of Google's photographic mapping activities in Canada began in March 2009 in 11 Canadian cities,[5] and the service itself was launched in Canada in October 2009. Visits to the website by Canadians more than doubled following the launch.[6]

Google announced on March 22, 2010 that it would be spending a few months photographing streets in cities and towns in all provinces and territories across Canada. Once finished, Canada will join the United States, United Kingdom, and France in having nationwide Street View. The company also said that it was returning to Windsor, Ontario, to reshoot the city, after city officials complained about the existing photos, which were taken during the long municipal workers' strike last summer. The photos taken in the spring had shown unkempt streets and garbage piles in many locations.[7]

Google Street View is now available throughout most of populated Canada, as shown on a map on the Google website indicating where Street View is available: http://www.google.com/intl/en_us/help/maps/streetview/where-is-street-view.html. This website also shows a sample of the areas in which Google's cars are currently operating.

Throughout 2009, the Privacy Commissioner of Canada was in discussions with Google Inc. to ensure that they were aware of Canada's privacy laws, and she expressed concerns about the camera surveillance required to set up the service. Following consultation with the Privacy Commissioner, Google agreed to blur faces and license plates in its Canadian Street View images.

---

4 CBC News, "Google Alerts Canadians About Street View Filming," CBC News Online, March 26, 2009, http://www.cbc.ca/technology/story/2009/03/26/tech-090326-google-street-view.html.

5 "Google Street View faces privacy roadblocks in Japan, Greece," CBC News Online, May 13, 2009, http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html.

6 Vito Pilieci, "Canadian Street View snoopers pump up Google's hits; Privacy concerns remain as more than 28 million images viewed in one day," *Ottawa Citizen*, October 10, 2009.

7 CBC News, "Google Street View to expand in Canada", CBC News, March 22, 2010, http://www.cbc.ca/technology/story/2010/03/22/google-street-view-windsor-canada.html.

The Google service already covers most of the United States, and has been introduced in more than 100 cities worldwide. The service has generated considerable controversy. For example, in May 2009, Greece's Data Protection Authority banned Google from taking Street View pictures in Athens until additional privacy safeguards, such as public notification of when the camera cars would be operating and additional storage security for the images had been implemented by the company.[8] In Japan, public complaints resulted in Google lowering its cameras by 40 centimetres to ensure that the images stay at eye level and do not peek over fences into private yards.[9]

In February 2010, European Union data privacy regulators issued a warning to Google that it must inform people before it sends cameras out into cities to take pictures for its Street View maps. The regulators also stated in a letter to Google that it should shorten the time it keeps its original photos from one year to six months. In a statement by way of response, Google said that its need to retain Street View images for one year is "legitimate and justified".[10]

In October 2010, Italy's privacy regulator announced restrictions on Google's Street View mapping service, echoing privacy concerns aired elsewhere in Europe. Google cars must now "be clearly identifiable by signs and stickers" indicating they will be taking pictures for Street View, the regulator said in a statement. Under the regulator's decision, Google must also publish on its website the names of the areas it intends to photograph three days ahead of time and publish the same information in at least two local newspapers and a radio station so residents can choose to avoid having their images collected. Google will be liable to fines of up to 180,000 euros for violating the new Italian rule, the regulator added.[11]

2. Privacy Protection

Google provides the following information regarding privacy protection to users on its website:

---

8 Derek Gatopoulos, "Google's Street View halted in Greece over privacy," *USA Today*, May 12, 2009, http://www.usatoday.com/tech/news/2009-05-12-google-street-view_N.htm. "Google Street View faces privacy roadblocks in Japan, Greece," CBC News Online, May 13, 2009, http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html.

9 "Google Street View faces privacy roadblocks in Japan, Greece," CBC News Online, May 13, 2009, http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html.

10 Aoife White "Google warned by EU over Street View map photos", *The Globe and Mail*, February 26, 2010, http://www.theglobeandmail.com/news/technology/google-warned-by-eu-over-street-view-map-photos/article1482311/.

11 "Italy privacy regulator orders restrictions on Google's Street View", *International Business Times*, October 26, 2010, http://www.ibtimes.com/articles/75777/20101026/google-street-view-italy.htm.

Public access only

Street View contains imagery that is no different from what you might see driving or walking down the street. Imagery of this kind is available in a wide variety of formats for cities all around the world. In select cases, Google will partner with an organization such as Disneyland Paris to schedule imagery collection of their property.

Street View images are not real time

Our images show only what our vehicles were able to see on the day that they drove past the location. Afterward, it takes at least a few months to process the collected images before they appear online. This means that images you look at on Street View could be anywhere from a few months to a few years old.

Individuals and license plates are blurred

We have developed cutting-edge face and license plate blurring technology that is applied to all Street View images. This means that if one of our images contains an identifiable face (for example that of a passer-by on the sidewalk) or an identifiable license plate, our technology will automatically blur it out, meaning that the individual or the vehicle cannot be identified. If our detectors missed something, you can easily let us know.

You can request removal of an image

We provide easily accessible tools allowing users to ask us to remove any images that feature inappropriate content (for example: nudity), or to remove any picture that features the user, their family, their car or their home. Below, you can review the steps to make a request.

How to Report a Concern

If you've found an image that you believe contains objectionable content, just follow these steps:

1. Locate the image in Street View.
2. Click "Report a problem" in the bottom-left of the image window.
3. Complete the form and click "Submit."

That's it. We'll review your report promptly.[12]

12 http://maps.google.ca/help/maps/streetview/privacy.html.

3. Google's Collection of Unsecured Wi-Fi Payload Data and the Office of the Privacy Commissioner's Preliminary Findings

Following a request from the German data protection authority in Hamburg to audit the Wi-Fi data collected by Google's Street View cars during a location-based project, Google discovered in May 2010 that it had been collecting payload data (the actual contents of transmissions made over a network) from unsecured wireless networks as part of its collection of information about Wi-Fi hot spots to support location-based services. A location-based service is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device.[13] By Google's own admission, it appears that this inadvertent collection was due to programming and code and software that it had developed with the purpose of collecting the Wi-Fi network data. As a result, Google halted the operation of its Street View cars, stopped the collection of Wi-Fi network data on May 7, 2010, and segregated and stored all of the data already collected.[14]

The Office of the Privacy Commissioner of Canada initiated three complaints against Google on May 31, 2010, pursuant to subsection 11(2) of PIPEDA,[15] after being made aware that Google Street View cars had been collecting payload data from unencrypted Wi-Fi networks during their collection of publicly broadcast Wi-Fi signals.

The three complaints are as follows:

a. Google's collection, use or disclosure of payload data was done without the individual's prior knowledge and consent;

b. Google's collection of payload data was done without prior identification of the purposes for which personal information (PI) was collected;

c. Google's collection of payload data was not limited to that which was necessary for the purposes identified.[16]

Following her investigation, on October 19, 2010 the Privacy Commissioner issued a *Preliminary Letter of Findings*[17] (Appendix B), which recommended that Google ensure it has a governance model in place to comply with Canadian privacy laws. The model

---

13 "Location-Based Services", GSM Association, January 2003, http://www.gsmworld.com/documents/se23.pdf.

14 Privacy Commissioner of Canada, *Preliminary Letter of Findings*, October 19, 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm.

15 Subsection 11(2) of PIPEDA states: "If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter."

16 Privacy Commissioner of Canada, *Preliminary Letter of Findings*, October 19, 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm.

17 Ibid.

should include controls to ensure that necessary procedures to protect individual privacy rights are duly followed before products are launched.

The Privacy Commissioner also recommended that Google enhance privacy training to foster compliance amongst all employees. As well, she called on Google to designate an individual or individuals responsible for privacy issues and for complying with the organization's privacy obligations—a requirement under Canadian privacy law.

She further recommended that Google delete the Canadian payload data it had collected, to the extent that the company does not have any outstanding obligations under Canadian and American laws preventing it from doing so, such as preserving evidence related to legal proceedings. If the Canadian payload data cannot immediately be deleted, the Privacy Commissioner recommended that it be secured and access to it be restricted.

The Privacy Commissioner will only consider the matter resolved upon receiving, either by or before February 1, 2011, confirmation of the implementation of the above recommendations, at which point she will issue her final report and conclusions.[18]

In an article dated October 22, 2010, *Associated Press* journalist Michael Liedtke reported that Google "is tightening its privacy leash on employees in an effort to ensure they don't intrude on people while the Internet search leader collects and stores information about its users."[19] According to Liedtke, "[b]esides promoting longtime employee Alma Whitten to be its director of privacy, Google said Friday that it will require all 23,000 of its employees to undergo privacy training. The company also is introducing more checks aimed at making sure workers are obeying the rules. Google's tougher privacy measures appear to be a response to recent breaches that have raised questions about the company's internal controls and policies." In his appearance before the Committee on November 4, 2010, Google Canada Policy Counsel Jacob Glick confirmed that these steps are being taken.

---

18 Ibid.

19 Michael Liedtke, "Google to impose tougher privacy measures after backlash to recent employee missteps, breaches," *Canadian Business Online*, October 22, 2010, http://www.canadianbusiness.com/markets/headline_news/article.jsp?content=b4951511?&page=2.

D. Canpages' Street Scene

1. The Service

A competitive service to Google Street View was launched by a Canadian online business directory company called Canpages, in partnership with an American company called MapJack.[20] Similar to the Google Maps Street View feature, Canpages' Street Scene offers panoramic street-level images of city streets, allowing users to explore whole neighbourhoods with a few clicks of a mouse. However, unlike Google Street View, Canpages' Street Scene focuses on commercial offerings. Indeed, as noted in a press release:

> Street Scene provides 360-degree street-level views of the city for people conducting local business searches on Canpages.ca. The technology enables users to pinpoint their search results on a map as well as see high resolution images of the results in the context of the local environment. For example, users can take a virtual "drive" down a city street to find out whether a restaurant offers parking or to see what a particular storefront looks like. [21]

Street Scene was launched in March 2009 for viewing Vancouver, Squamish and Whistler online.[22] In August 2009 Canpages photographed the downtown cores and commercial arteries of Toronto[23] and Montreal,[24] and both cities are now online.

---

20 Kris Abel, "Canada AM—Street View Comes to Canada With New Tricks From CanPages.ca," CTV.ca—Kris Abel's blog, March 16, 2009, http://krisabel.ctv.ca/post/Canada-AM-e28093-Street-View-Comes-To-Canada-With-New-Tricks-From-CanPagesca.aspx. Canpages is the largest independent local search and directories publisher in Canada. Its website, Canpages.ca features a national residential and business database and more than 3.5 million unique visitors come to visit it every month with their local search requests. With 80 publications and over 80,000 customers, Canpages reaches more than 8 million households and businesses across Canada. Headquartered in Vancouver, Canpages employs approximately 700 people and has offices in Alberta, British Columbia, Ontario and Quebec: http://corporate.canpages.ca/about_us/company_profile/where_local_search_gets_done.

21 Canpages Inc., "Canpages to Begin Street Scene Shooting in Toronto", August 11, 2010, http://corporate.canpages.ca/media/Street%20Scene%20Toronto%20Shoot.pdf.

22 Kris Abel, "Canada AM—Street View Comes to Canada With New Tricks From CanPages.ca," CTV.ca—Kris Abel's blog, March 16, 2009, http://krisabel.ctv.ca/post/Canada-AM-e28093-Street-View-Comes-To-Canada-With-New-Tricks-From-CanPagesca.aspx.

23 Canpages Inc., "Canpages to Begin Street Scene Shooting in Toronto", August 11, 2009, http://corporate.canpages.ca/media/Street%20Scene%20Toronto%20Shoot.pdf, and Kenyon Wallace, "Google Street View gets Canpages competition", *Toronto Star*, August 11, 2009, http://www.thestar.com/business/companies/google/article/679194--google-street-view-gets-canpages-competition.

24 Roberto Rocha, "Canpages Street Scene launches in Montreal", *Montreal Gazette*, August 27, 2009, http://www.canada.com/montrealgazette/Canpages+Street+Scene+launches+Montreal/1936073/story.html.

2. Privacy Policy

Canpages' privacy policy[25] states the following regarding Street Scene:

> In providing Canpages Street Scene Service, Canpages has been sensitive to avoid including photographic information which would provide personal information about identifiable individuals. We are sensitive to the privacy concerns that might be raised by individuals who were photographed during the preparation of the data required by the Street Scene service. Photographs of identifiable individuals are in no way required by the service. The assembly of the data is designed to deliberately blur the faces of any individual who may be photographed in this process. You will notice as a result that no individual can be identified while using the Mapjack service. If you wish to report a privacy concern, please do so by clicking the "report a concern" on one the Street Scene Service Page.

The privacy policy also contains a statement specifying that "Our privacy policies follow the 10 principles of fair information practices as described by the Privacy Commissioner for Canada". The 10 principles are then listed:

a. Accountability: An organization is responsible for personal information under its custody and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

b. Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

c. Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

d. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

e. Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

f. Accuracy: Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

g. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

h. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

i. Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to that

---

25 Accessible online at: http://www.canpages.ca/hm/privacy.jsp.

information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

j. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

3. Canada Eye

In March 2010, Canpages launched a free "augmented reality" iPhone application for local search called the Canada Eye. Canada Eye lets users search and view the direction and distance to all specific business locations in real-time overlaid on iPhone's screen. "Augmented reality" is the latest technology coined for applications that leverage the iPhone 3GS' compass, GPS and video camera simultaneously. As noted in a press release, "the Canpages application enables users to search for a specific business category-from local delis and mom and pop bakeries to Starbucks and Tim Hortons-and then shows the direction and distance to all of the businesses in the category in the local area. Essentially, Canada Eye is one application that allows users to locate businesses nearby as well as how to get to them in real time."[26]

In June 2010, Yellow Pages Group acquired Canpages for approximately C$225 million.[27]

WHAT THE COMMITTEE HEARD: INITIAL TESTIMONY ON GOOGLE AND CANPAGES' STREET-LEVEL IMAGING APPLICATIONS

A. Google Canada

Jonathan Lister, Managing Director and Head of Google Canada, appeared before the Committee on June 17, 2009. In his introductory remarks Mr. Lister emphasized how Google Street View "is a product that is changing the way people think about maps... The great innovation of Google Street View is the ability to marry street-level images with digital maps in order to provide a superior product for Internet users".[28]

With regard to the legal and privacy obligations incumbent upon Google as it operates in different countries, Mr. Lister stated the following:

---

26 "Canpages Brings 'Augmented Reality' Local Search to the iPhone 3GS", March 10, 2010, http://www.benzinga.com/pressreleases/m166514/canpages-brings-augmented-reality-local-search-to-the-iphone-3gs.

27 Yellow Media Inc., *Yellow Pages Group Finalizes Acquisition of Canpages*, June 23, 2010, http://corporate.canpages.ca/media/Yellow%20Pages%20Group%20Finalizes%20Acquisition%20of%20Canpages.pdf.

28 Jonathan Lister, *Evidence*, Meeting No. 29, June 17, 2009, at 1550, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=E&Mode=1&Parl=40&Ses=2.

> First and foremost, Google is respectful of the laws of each country in which Street View operates. The imagery we make available shows no more than what any of you would see while travelling down a public street. The images in Street View are a snapshot in time, often several months to a year old. They aren't real time. While we only collect images from public places, we've always recognized that some passers-by may be inadvertently included in our pictures. As such, Google has invested significant resources into the development of a world-leading process for identifying and blurring certain features in an image, namely, identifiable faces and licence plates[...].
>
> Another key component to the privacy protections built into Street View is the easy-to-use, take-down request system. Every published Street View image includes a "report a problem" link, which takes users to a simple removals page. Any individual can ask to have an image entirely removed from the publication if it features themselves, their family, their car, or their home. This removal applies even if aspects of the image have already been blurred. We process removal requests every day in multiple languages and offer a fast and efficient turnaround time for each request.
>
> Another important aspect of our efforts to ensure privacy protection is our commitment to work with key stakeholders in every country in order to identify and contact relevant local organizations prior to launch. Our team will work to reach out to Canadian stakeholders and provide them with all the relevant details of Street View, including how to have their organization's image removed or blurred from the site.
>
> We're also putting in place a system that will ensure that on launch day for Street View in Canada, we will have additional staff on hand to handle take-down requests.
>
> Let me close by saying that as with many cutting-edge technologies, the challenge we face with Street View is striking the right balance between building a sophisticated and highly useful tool and ensuring that the data we collect to provide these services is used appropriately.[29]

Mr. Lister's June appearance before the Committee was prior to the Canadian launch of Street View in October 2009. At that time he informed the Committee that Google was working closely with the Privacy Commissioner's office in order to ensure that its privacy and legal obligations were met prior to Street View's launch.[30] In response to concerns about the capacity of Street View to invade the privacy of individuals within their homes or to see inside sensitive spaces such as women's shelters, Mr. Lister emphasized that Street View images are taken of the exterior of public places: "[T]he intended use [of Street View] is to improve mapping and capture the façades of publicly accessible, available buildings and landmarks. There is no need to see inside; it's not in the product definition to do that, and Google doesn't do it."[31]

With regard to the storage and disposal policies, Google images are held at secure "server farms," most of which appear to be in the United States.[32] With respect to the original unblurred images, Mr. Lister stated that Google retains non-blurred images for

---

29 Ibid.

30 Ibid. at 1605, 1650.

31 Ibid. at 1630.

32 Ibid. at 1625.

product enhancement, such as improving the blurring technology's recognition capacities. He added that Google had decided to revise its data retention policy to keep unblurred images for an "adequate but non-excessive period of time", after which non-blurred images would be permanently blurred and thus rendered anonymous (rather than disposed of).[33] As of June 2009, Google had not determined the exact timeframe for retention of the unblurred images.[34] He indicated that he would share this timeframe with the Committee once Google has a "reasonable and accurate answer".[35] Following Mr. Lister's appearance before the Committee, agreement was reached between Google and the Office of the Privacy Commissioner that Google would retain the unblurred images for the period of one year.[36]

B. Canpages

In his appearance before the Committee on June 17, 2009, Mr. Olivier Vincent, President and Chief Executive Officer of Canpages, explained the function of Canpages Street Scene, which focuses on commercial areas: "Fully integrated with Canpages' local search functionality, Street Scene provides panoramic street-level views of the city, so users can not only pinpoint their search results on a map, but also see high-resolution visuals of their search results in the context of the local environment. For example, users can take a virtual walk down the city streets to a local restaurant or hotel. They can see how it looks from the outside before they make a reservation, or they can assess where there is street parking or some other parking lot nearby."[37]

With regard to the privacy concerns raised by Street Scene's use of images and imaging technology, Mr. Vincent stated the following:

> Canpages considers respect of privacy as a key priority and is sensitive to the privacy concerns that might be raised by individuals who are photographed during the preparation of the data required by the Street Scene service. Canpages is committed to bringing every individual the assurance that it will respect their privacy, and has publicly stated its privacy policy regarding its Street Scene service.
>
> We will notify the public before we start shooting. Individual faces and other recognizable features like licence plates are blurred on the captured image prior to being posted online. The blurring process uses a proprietary technology that is irreversible by the users. All original non-blurred files are destroyed after blurring and before being posted online. There is no way to get back these original files later on.

---

33 Ibid. at 1610.

34 Ibid. at 1650.

35 Ibid. at 1715.

36 Elizabeth Denham, *Evidence*, Meeting No. 32, October 22, 2009, at 0930, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=E

37 Olivier Vincent, *Evidence*, Meeting No. 29, June 17, 2009, at 1555, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=E&Mode=1&Parl=40&Ses=2.

> Users can report any concern at any time using the "report a concern" feedback located on every image. Upon a specific request, Canpages will provide extra blurring for an entire person, a vehicle, a window, a building, a pet—you name it. While privacy laws are not necessarily reflective of the rapidly growing field of technology, we at Canpages want to take a proactive approach to all concerns that may be raised.
>
> [...]
>
> Canpages has engaged with the public, the privacy commissioners of Canada, and Mr. Pierre Poilievre, the MP who filed a motion before this committee to review privacy matters.
>
> In conclusion, Canpages is committed to working both immediately and as part of an ongoing process to address potential privacy issues that might arise as a result of its continuous innovation in the field of local search.[38]

Following his introductory remarks, Mr. Vincent discussed, among other topics, the company's blurring technology for protecting the anonymity of passers-by and sensitive places. He testified that while earlier versions of blurring technology were more easily reversed, the new version his company is using is much stronger and cannot be reversed. He also testified that the original versions of any images which require blurring are destroyed and replaced by the blurred version once the technology has been applied.[39]

C. Office of the Privacy Commissioner of Canada

Elizabeth Denham, Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada, appeared before the Committee on October 22, 2009. Ms. Denham informed the Committee that PIPEDA is a technology-neutral law that is a "dynamic, modern, and effective tool for strengthening the privacy rights of Canadians" that was designed to respond to such situations as the "commercial collection and use of personal information through street-level imaging technology".[40] While aware that the many services that use street-level imaging are very popular with the public, the Office of the Privacy Commissioner remains concerned about ensuring that the commercial use of the technology "protects the privacy of Canadians by meeting the requirements of PIPEDA, such as knowledge, consent, safeguards, and limited retention."[41]

The view of the Office of the Privacy Commissioner is that citizens should know in advance that street-level images are being taken, when, and why, and how they can have their image removed if they don't want it to appear online. Faces and license plates need to be blurred so that the individual is made anonymous or is at least not identifiable. Companies need an effective and quick take-down process whereby an individual can

---

38 Ibid.

39 Ibid., at 1620, 1625 and 1720.

40 Elizabeth Denham, *Evidence*, Meeting No. 32, October 22, 2009, at 0900, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=E.

41 Ibid.

have their image removed. Unblurred images retained for legitimate business purposes should be protected with appropriate security measures and the raw data should not be retained indefinitely.[42]

Ms. Denham observed that improvements have been made in these areas by the service providers who appeared before the Committee. In August 2009, Google agreed with the Office of the Privacy Commissioner and with other data protection commissioners in Europe that they needed to delete unblurred imagery after one year. As per her testimony:

> One of the most contentious issues that we had in our discussions with Google and Canpages is what happens to the raw imagery, the unblurred imagery that's stored in databases in the U.S. At first Google was very reluctant to set a retention period for how long they were going to keep that data. In August they agreed with us and they agreed with other data protection commissioners in Europe that indeed they needed to delete the unblurred imagery after one year. They gave us the business rationale as to why they needed to keep it for a year. We accepted that. We also have an undertaking from Google that we can visit their facilities and review how they are permanently deleting or permanently anonymizing the data after a year. That was one of our major concerns with the service.[43]

Ms. Denham also told the Committee that since the launch of Google Street View at the beginning of October 2009, the Office of the Privacy Commissioner had received fewer than a dozen inquiries from Canadians, and only one complaint, which was resolved. This complaint concerned an individual who felt that his image had been captured. The complaint was resolved during the investigation by Google agreeing to permanently delete the man's image from the database, so the Privacy Commissioner never issued a public recommendation. The Office of the Privacy Commissioner had not received any complaints regarding the effectiveness of Google's take-down procedure by the time of Ms. Denham's appearance before the Committee. The Office of the Privacy Commissioner had received calls from individuals asking how to remove their images from Street View. These individuals were referred to Google, and none of them has subsequently returned to the Office of the Privacy Commissioner with a full-scale complaint so far.[44]

In response to a question as to whether the Office of the Privacy Commissioner is satisfied that Google's blurring policy meets the standards found in Canadian commercial privacy laws, Ms. Denham replied that she believes that Google could do a better job with their blurring technology: "We were told by Google that their blurring technology was 98% effective; that was before the images went live. But we've seen for ourselves that there are many instances in which individual faces are not blurred. Google is committed to continuing to improve the blurring, which is one of the reasons they want to retain the

---

42 Ibid. at 0905.

43 Ibid. at 0930.

44 Ibid. at 0930, 1025.

images for one year. They're working on improving their blurring technology." The Privacy Commissioner is satisfied with the one year timeframe.[45]

WHAT THE COMMITTEE HEARD: FOLLOW-UP TESTIMONY ON GOOGLE'S COLLECTION OF WI-FI DATA

A. Office of the Privacy Commissioner of Canada

Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada, appeared before the Committee on October 28, 2010, to speak about the Office's investigation into Google's collection of Wi-Fi data that culminated in the Office's *Preliminary Letter of Findings* released on October 19, 2010.[46] She also provided updates regarding the privacy implications of street level imaging technology. She was accompanied by Daniel Caron, Legal Counsel (Legal Services, Policy and Parliamentary Affairs Branch), and Andrew Patrick, Information Technology Research Analyst.

In her opening statement, Ms. Kosseim summarized the office's investigation into Google's inadvertent[47] collection of unsecured Wi-Fi payload data with its Street View cars. As she explained, payload data is information about the communications that run through Wi-Fi networks.[48] The Privacy Commissioner's investigation found that:

> [...]Google had inappropriately collected personal information of Canadians from unsecured wireless networks. In some cases, that personal information was highly sensitive, including complete e-mails, user names and passwords, and even medical conditions of specified individuals. Unfortunately, this collection of data was due to an error that could have been easily avoided if Google's own procedures had been followed.
>
> Essentially what happened here was the engineer who developed the code to sample categories of publicly broadcast Wi-Fi data also included code allowing for the collection of payload data, thinking that this type of information might be useful to Google in the future. The engineer had identified what he believed to be "superficial" privacy concerns, but contrary to company procedure, failed to bring these concerns forward to product counsel, whose responsibility at Google would have been to address and resolve these concerns prior to product development.[49]

As noted earlier in the report[50], the Privacy Commissioner recommended that Google re-examine and improve the privacy training it provides to all its employees and

---

45 Ibid. at 1025.

46 Privacy Commissioner of Canada, *Preliminary Letter of Findings*, October 19, 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm.

47 As described by Patricia Kosseim.

48 Patricia Kosseim, *Evidence*, Meeting No. 28, October 28, 2010, at 1535, http://www2.parl.gc.ca/HouseePublications/Publication.aspx?DocId=4739584&Language=E&Mode=1&Parl=40&Ses=3.

49 Ibid.

50 See "Google's Collection of Unsecured Wi-Fi Payload Data and the Office of the Privacy Commissioner's Preliminary Findings".

ensure that it has an overarching governance model in place that guarantees that procedures to protect privacy are followed prior to the launch of any product. Furthermore, the Privacy Commissioner called on Google to delete the Canadian payload data it collected to the extent that it is able to do so under Canadian and U.S. laws.[51]

Ms. Kosseim explained that the Privacy Commissioner issued a *Preliminary Letter of Findings* with regard to Google's collection of Wi-Fi data as she is seeking proof and evidence that the recommendations will actually be followed before she formally concludes, or "resolves", her investigation. In other words, the Privacy Commissioner is seeking "actual implementation and not just undertakings".[52]

Ms. Kosseim then detailed how the Office of the Privacy Commissioner initially became aware that Google was collecting Wi-Fi signal and payload data. She testified that the office had received notice from Google in April 2010 "that they had intended and they were collecting publicly broadcast Wi-Fi radio signals." [53] Google had explained that this was in order for the company to be able to enhance its offering of "location-based services". [54]

Ms. Kosseim further explained that while the collection of the Wi-Fi signals was not related to the Google Street View product itself, as a matter of practicality, Google used the Street View cars in order to collect the Wi-Fi data. Indeed, Google told the Office of the Privacy Commissioner in April 2010 that they were putting antennae on the roofs of the Street View cars to at the same time collect and capture the neighbouring Wi-Fi radio signals.[55]

Only in May 2010, after being prompted by requests for further information from German data protection authorities, did Google realize that it was unknowingly collecting Wi-Fi payload data.[56] As detailed in the *Preliminary Letter of Findings*, on May 7, 2010, Google grounded its Street View cars, stopped the collection of Wi-Fi network data, and segregated and stored all of the data already collected.

---

51 Patricia Kosseim, *Evidence*, Meeting No. 28, October 28, 2010, at 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4739584&Language=E&Mode=1&Parl=40&Ses=3.

52 Ibid. at 1540.

53 Ibid. at 1555.

54 Ibid. As described earlier in the report, a "location based service" is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device.

55 Ibid.

56 Ibid.

The Office of the Privacy Commissioner had no reason to believe, from the basis of the investigation, that there was anything untoward done with the Wi-Fi payload data that had been inadvertently collected by Google.[57]

Nonetheless, the Office of the Privacy Commissioner recognized that the mere collection of information about Wi-Fi access or location points can itself raise potential privacy concerns. As noted by Mr. Andrew Patrick: "[I]f information about the presence of a Wi-Fi access point can be at all linked to a particular individual, either individually or in combination with other bits of information, then it would be potentially personal information and therefore potentially something that we would be worried about."[58] The office does not have specific information about the actual location-based services that Google is developing with the collection of Wi-Fi radio signals.[59]

Overall, Patricia Kosseim expressed confidence that Google will implement the Privacy Commissioner's recommendations contained in the preliminary letter of findings:

> I think we have every indication to be confident. Again, there has been, not formal responses to us from Google, but responses in the press that we have heard, as all of you have, to indicate concrete steps that they have already taken and steps that we have learned of in the course of our investigation had already been undertaken to begin the process of putting in place appropriate governance structures within the organization which is a global giant as you can understand. The date of February 1 was deliberately chosen bearing in mind a reasonable amount of time that it will take not only to undertake to make these changes but to have concrete evidence that they've been made at a global scale. That's why the date was given. We have every hope that we will get a positive response earlier than that and we'd be delighted to do so. We are fairly confident that there will be a good ending to this.[60]

As well, Ms. Kosseim noted that at this time the Office of the Privacy Commissioner is satisfied with the privacy protections found in the Google Street View and Canpages Street Scene technologies, which are separate from the incident regarding the collection of Wi-Fi payload data:

> In respect of the Street View imaging technology by Google and Canpages, one point I just want to clarify is that those were never the subject of an investigation by the commissioner...on the basis of the correspondence and the response of the organizations, there has been a lot of movement on the part of both organizations to comply with or to move along in harmony with the recommendations that the commissioner has made including notification to neighbourhoods before they arrive, discussions with vulnerable stakeholders and groups, take down procedures, retention and deletion mechanisms and other such protections. So it's on the basis of that correspondence there's been a lot of movement. Of course there could always be improved notification, there could always be ongoing improvements to blurring

---

57 Ibid. at 1605.

58 Ibid.

59 Ibid. at 1610.

60 Ibid.

technology but so far there's been great improvement and movement towards the commissioner's wishes.[61]

In conclusion, Ms. Kosseim emphasized one over-arching recommendation to companies such as Google, Canpages and Facebook that use new technologies to compile, process and share information in various ways, namely that such organizations must adopt the precautionary principle with regard to the possible privacy implications of new technologies. It is the hope of the Office of the Privacy Commissioner that organizations, when conceiving, developing, and deploying information technologies of which Canadians all benefit "take the proactive measures up front to identify the risks, asses them, and manage them before deployment of these technologies on a widespread basis."[62]

B. Google Canada

1. Appearance of Jacob Glick on November 4, 2010

In his appearance before the Committee on November 4, 2010, Mr. Jacob Glick, Canada Policy Counsel for Google Inc., spoke both about Google Street View and about Google's collection of Wi-Fi payload data.[63]

With regard to Street View, Mr. Glick noted that Google has "addressed all of the concerns identified by this committee and by the Privacy Commissioner. We've implemented the most sophisticated blurring technology to blur faces and licence plates in all of our images. We've implemented a quick and easy take-down procedure. Anybody can request that Google remove pictures of themselves, their house, their kids, or their car, from Google Street View. Finally, we are permanently baking in this blurring after one year."[64] Mr. Glick noted that Canadians are avid users of Street View. Indeed, "in absolute numbers, Canadians are the third most active users of Street View in the world, behind only the U.S. and the U.K. Since its launch, Canadians from coast to coast to coast have used this next generation cartography to map their way to the store, promote their local business, sell their house, and explore our country online."[65]

With regard to Google's collection of Wi-Fi payload data, Mr. Glick clarified that it was not related to the Street View product, but that Street View vehicles were used as a platform for the collection. He apologized on behalf of Google for what had happened, noting that "what happened is not consistent with our commitment to serving Internet

---

61 Ibid. at 1705.

62 Ibid. at 1705.

63 Jacob Glick, *Evidence*, Meeting No. 30, November 4, 2010 at 1530, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4764635&Language=E&Mode=1&Parl=40&Ses=3.

64 Ibid.

65 Ibid.

users".[66] He emphasized that "no payload data transferred over encrypted networks was collected by Google. Google had no desire to use payload data in any way. No payload data has been used in any Google product or service, and none of the Canadian payload data has been given or disclosed to third parties; it has been segregated and secured."[67]

In terms of how Google Street View cars came to collect Wi-Fi payload data, Mr. Glick testified that at the time that Google was preparing to launch Street View and was deploying a fleet of vehicles around the world to collect street level imaging in 2007, a Google engineer had the idea of using Street View vehicles as a platform to detect Wi-Fi hot spots to support location-based services:

> Using publicly broadcast Wi-Fi hot spots as landmarks to help users identify where they are is common industry practice. The engineer designed software code to collect Wi-Fi network data, and unfortunately, also Wi-Fi payload data. Payload data refers to the contents of transmissions. Google did not want this payload data and does not believe that collecting such payload data is useful or appropriate. The engineer should have flagged, for Google's in-house lawyers, the plan to collect Wi-Fi payload data. He did not do so. If he had, this would have been an opportunity at the outset of the program for Google to identify the problem and stop it. As a result, the code was deployed on Street View vehicles. The software worked as it was programmed to do, collecting Wi-Fi network data and Wi-Fi payload data sent over un-encrypted networks.[68]

In April 2010, Google was asked by German authorities to audit the Wi-Fi data collected by Street View vehicles. This audit revealed that Google had been collecting Wi-Fi payload data in addition to the network data. According to Mr. Glick, "[b]efore announcing publicly what we discovered, I personally called Commissioner Stoddart and advised her of this issue. After that, Google made a public announcement and apologized for what had happened."[69] Street View vehicles were grounded, and data was segregated. According to Mr. Glick, "nobody has reviewed the Canadian payload data, other than the Privacy Commissioner's investigators and those who facilitated their investigation. It has not been disclosed to any third parties."[70] It was not clear from Mr. Glick's testimony whether the Wi-Fi data collection only began in April, or whether it began beforehand.

Mr. Glick confirmed that on October 22, 2010 Google made a number of significant changes to its privacy policies and controls. Mr. Glick indicated that he had spoken with Commissioner Stoddart prior to the public announcement of the following measures:

> [F]irst, Google appointed Dr. Alma Whitten as our director of privacy to ensure we build effective privacy controls into our products and internal practices. Dr. Whitten is an internationally recognized expert in the computer science field of privacy and security. Second, we are enhancing our core privacy training with a particular focus on the responsible collection, handling, and use of data. Finally, Google is adding new

---

66 Ibid.

67 Ibid.

68 Ibid.

69 Ibid.

70 Ibid.

> safeguards to our existing privacy-compliant system to include independent internal audits to ensure that user privacy is protected.[71]

Google is of the view that these changes will significantly improve its processes and controls to prevent something like the Wi-Fi incident from happening again.

Mr. Glick was asked numerous times about how the position of Director of Privacy will work at Google and about Dr. Alma Whitten's qualifications for the position.[72] While Mr. Glick was not able to provide a biography of Dr. Whitten at the time, he noted that she has been at Google for a number of years, that her doctorate is in the area of computer science and security, and that she has published numerous papers on computer science, security and privacy. She has been a leader in the area of privacy and security on a global basis for a number of years. She is based in the London, England office of Google.[73]

Based on Mr. Glick's testimony, it would appear that Google had not yet disposed of the Canadian payload data that it had collected, as it was unclear whether it had to be preserved for some reason.[74] Mr. Glick undertook to verify whether and when the Canadian payload data would be deleted,[75] and whether there might be any impediment under U.S. law with regard to the deletion of that information.[76]

2. Appearance of Jacob Glick and Alma Whitten on November 25, 2010 (via teleconference)

Following Mr. Glick's appearance on November 4, 2010, the Committee decided to hear from Google's new Director of Privacy, Dr. Alma Whitten, as well as Mr.Glick, on November 25, 2010, seeking further information on the initiatives being undertaken by Google following the Wi-Fi data incident, and in response to the Privacy Commissioner's *Preliminary Letter of Findings* released on November 19, 2010. Both witnesses appeared via teleconference, Dr. Whitten testifying from London, England, and Mr. Glick testifying from Toronto.

Prior to her appearance, Google sent the Committee the following biography of Dr. Whitten:

> Alma Whitten joined Google in 2003 and currently serves as the company's Director of Privacy for both the engineering and product teams. In this role, she will ensure Google builds effective privacy controls into user products and internal practices. An internationally-recognized expert in privacy and security, Alma has testified before the

---

71 Ibid.

72 See for example at 1550 and 1555.

73 Ibid. at 1550.

74 Ibid. at 1600.

75 Ibid.

76 Ibid. at 1635.

U.S. Congress and has appeared before the European Commission's Article 29 Working Party.

Previously, Alma served first as Lead for Google's Applied Security engineering team, and then as Google's Privacy Engineering Lead where she grew teams that developed tools like the Google Dashboard.

Prior to joining Google, Alma was best known for her 1999 technical paper on usability as a primary issue for computer security, titled "Why Johnny Can't Encrypt," which is recognized as a founding paper for usability of security as a field of research. She continues to research, write, and speak on human-centered approaches to security and privacy as part of her work at Google. Alma holds a Ph.D. in Computer Science from Carnegie Mellon University.[77]

In her testimony to the Committee, Dr. Whitten noted that: "I've devoted my career both as an academic and now as Google's Director of Privacy to one primary goal: to make it intuitive, simple, and useful for Internet users to take control of their privacy and security,"[78] and she spoke about Google's plans to strengthen its internal privacy and security practices:

> With my expanded responsibilities, I will have the chance to oversee and work with both the engineering and the product teams to help ensure that privacy and security considerations are built into all of our products. While the duties that go with this role are big, I am confident that I will be supported with the resources and internal support needed to help Google do better... We want to make certain that each product we roll out meets the high privacy and security standards that our users expect of us.[79]

She explained that Google will be providing privacy training to its employees tailored to their various responsibilities[80], including broad security and privacy compliance training, code of conduct compliance training, and a more focused and deeper training specific to different kinds of job roles:

> A very important point we will be making over and over again in our training is that individual engineers should never be making these judgment calls by themselves. We want to educate them on the privacy landscape and privacy concerns.
>
> We want to very much educate them on Google's own articulated privacy principles of transparency, control, and responsible stewardship above all, but we also want to educate them very, very strongly and reinforce that education in many ways on the improved processes we are putting in place, to make sure that those fail-safes are there, that the thoughtful review is in place, and that individual engineers don't try to "lawyer" questions by themselves.

---

77 E-mail letter to the Clerk of the Committee, November 22, 2010. Further information on Dr. Alma Whitten can be accessed at: http://www.google.com/research/pubs/author32149.html.

78 Dr. Alma Whitten, *Evidence*, Meeting No. 34, November 25, 2010, at 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Language=E&Mode=1&Parl=40&Ses=3.

79 Ibid. at 1540.

80 Ibid. at 1600.

[...]

> For newly hired engineers, we expect to give them a significant session of privacy training within their first two weeks at the company, before they would be writing any code, before they would be starting on any product development. With that initial training, we expect to lay a lot of the seeds in place in putting the framework in place for them to know who they are supposed to talk to and when, to know where the resources are internally to help them understand privacy and to understand our privacy processes, and where those are quickly and easily found--all of those aspects of who they should talk to.
>
> For engineers going forward, for the people who aren't going to be hired next week or the week after that to come in through this initial training, we will be doing follow-up training. But above all, I think, the process, which we are enhancing and optimizing now, and the training have to really be two halves of the same coin that will reinforce each other and work closely together.
>
> The process will force engineers to engage with the training at various parts of their project's life cycle. As they are expected to engage with the process, then the training is there to tell them how to do so and to provide them help to enable them to do so. The goal is very, very much for those two aspects to strongly reinforce each other to make this as effective as possible.[81]

Dr. Whitten also explained how Google ensures that it has expertise in the privacy considerations of the various countries where it operates:

> We do have local expertise on the ground in as many countries as possible--in fact, in most countries. I spoke to the earlier question from the member about the need to bring in all of these different kinds of expertise across legal and engineering functions.
>
> We're also very conscious of that cross-culturally, and of the need for our privacy review to bring in perspectives from all of the different parts of the world where our products are going to be seen, used, and experienced. That's part of the reason why I am now based in Europe: to make sure that even in my own person I can bring in a little bit of extra balancing, having started out in the United States and then bringing that over there.
>
> Canada is certainly one of the countries where we pay very, very close attention to the work of your Privacy Commissioner and to her voice on the international stage. We rely very heavily on Jacob's relationship and close communications with her office. We do similar things in all of the countries where we're present.[82]

In his testimony before the Committee on November 25, 2010, Mr. Glick confirmed that Google had not yet deleted the Canadian Wi-Fi data that it had collected, pending analysis of any issues that may prevent the immediate deletion of the data:

> What we're doing is precisely what the Privacy Commissioner asked, which is undertaking an analysis of Canadian and U.S. law, both in terms of the laws of evidence and other applicable laws, to determine the extent to which it can be deleted. In the

---

81 Ibid. at 1625.

82 Ibid. at 1645.

interim we're doing precisely what she asked, which is maintaining the safeguards around the data and the protections for it.[83]

Mr. Glick added that "ultimately our objective here is to, as I've said before, delete all of the data. We didn't want it in the first place, we don't want it now, but we don't want to prematurely delete it and cause more headaches."[84] He undertook to provide the Committee with a list of countries where Google has been subject to criminal charges or administrative penalties with respect to the collection of Wi-Fi payload data.[85]

In a letter to the Committee dated December 9, 2010, Mr. Glick provided the following responses to the Committee's questions:

1. In what countries was payload data from unencrypted Wi-Fi networks mistakenly collected by Google:

United States of America, Canada, much of Europe (Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Great Britain/UK, Greece, Hungary, Ireland, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden and Switzerland), Australia, Hong Kong, Japan, South Korea, Macau, New Zealand, Singapore, Taiwan, Brazil, Mexico and South Africa.

2. Where has the payload data been stored:

Payload data collected anywhere in the world prior to May 2010, when this problem was discovered and the payload collection ceased, was and is stored in the United States.

Hard drives from street view vehicles that were not processed by the time we learned of the problem have been secured on a regional basis. Hard drives from North America, South America and Asia are in the United States. Hard drives from Europe and Africa are in Europe.

3. What payload data has been deleted:

Payload data identified as being from the following countries has been securely deleted as of the date of this letter: Ireland, Austria, Denmark, Hong Kong and the United Kingdom.

4. Has Google faced criminal charges or administrative penalties or sanctions related to this matter anywhere around the world?

No.[86]

---

83 Jacob Glick, *Evidence*, Meeting No. 34, November 25, 2010, at 1605, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Language=E&Mode=1&Parl=40&Ses=3.

84 Ibid. at 1620.

85 Ibid. at 1715.

86 E-mail letter from Jacob Glick to the Committee, December 9, 2010.

C. Yellow Pages Group (Canpages)

On November 25, 2010 the Committee also heard testimony from François D. Ramsay, Senior Vice-President, General Counsel, Secretary and Responsible for Privacy, and Martin Aubut, Senior Manager, Social Commerce, in order to learn about any updates regarding the Yellow Pages / Canpages Street Scene product, and to determine how the company incorporates privacy considerations into the development of its products.

In his opening statement, Mr. Ramsay provided a brief introduction of Yellow Pages Group, which acquired Canpages in June 2010. He clarified that the Street Scene product licenses its map data from two companies, MapJack and Google. Following Google's discovery regarding the collection of Wi-Fi payload data, Yellow Pages Group obtained confirmation from MapJack that it had never collected either Wi-Fi network or payload data:

> Depending on where you are within our universe of websites, [Yellow Media Inc., the network of companies that include Yellow Pages Group, Trader Corporation, and Canpages is] currently using Street View technology from Google and Microsoft, in addition to MapJack, the provider that Canpages has historically used.
>
> I am pleased to confirm to the committee that Canpages' supplier of the Street Scene service, MapJack, has not been used to collect either Wi-Fi network data or Wi-Fi payload data. Therefore, we have never been in possession of any such data.
>
> Yellow Media Inc., YPG, Trader, and Canpages are fully committed to abiding by the privacy legislation applicable to our business.[87]

Mr. Ramsay and Mr. Aubut indicated that they could provide the Committee with confirmation of the types of technology used by their contractors for Canpages products.[88]

With regard to privacy training provided for employees of Yellow Pages Group, Mr. Ramsay noted that until now no such training had existed. However, given his appearance before the Committee, and upon hearing the testimony of Google's Dr. Alma Whitten, he is going to look into how Yellow Pages Group can provide privacy training for its employees.[89]

As well, Mr. Ramsay noted that Yellow Pages Group has not historically had direct contact with the Privacy Commissioner of Canada to consult on potential privacy issues regarding products. This is something that he is interested in changing, as he testified, "I've determined with some of my colleagues that this is something that we'd be interested in exploring and being proactive about. We understand that as the world becomes more

---

87 François Ramsay, *Evidence*, Meeting No. 34, November 25, 2010, at 1530, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Language=E&Mode=1&Parl=40&Ses=3.

88 Ibid. at 1710.

89 Ibid. at 1630.

digital, obviously, many of these issues will come to the forefront. It's important for us to be on top of these matters and to be responsive and proactive on legitimate privacy concerns that Canadian institutions have."[90]

With regard to Canada Eye, a geolocation based service launched by Canpages in March 2010, Mr. Ramsay explained the following:

> I don't know if some of the members here have iPhones, but there is a button on the Canpages application that you can use. I'm more familiar with another one from a competitor of Canpages, YPG. Basically, you use the camera feature of your iPhone, pointing in a direction, and listings are pushed using the GPS features of the iPhone or the smartphone that you're using. [...] The image is a bit of a gimmick, I guess, in the sense that it's not really the eye that is seeing. It's just that the iPhone understands in which direction it is pointing and therefore understands which businesses are located in the direction in which you are pointing.
>
> So just to confirm, it's not strictly speaking the fact that the camera sees a business that it identifies it. It's just that it's geo-coded. The businesses are geo-coded, and the phones pointing in that direction push the listing that is being provided.[91]

To the best of Mr. Ramsay's knowledge, smartphone services such as Canada Eye are consistent with Canadian privacy legislation and policies. He noted that "the service we're using to provide directions for people is, again, with services that are provided by the likes of Google and Microsoft."[92] In other words, it does not seem that the geolocation technology was developed in-house by Yellow Pages Group.

CONCLUSION

The Committee, after hearing evidence from Google Canada, Canpages, and from the Office of the Privacy Commissioner of Canada, is satisfied that the privacy concerns of Canadians with regard to street level imaging technology are being taken seriously by all parties involved. Best practices have been developed by Google and Canpages, in consultation with the Office of the Privacy Commissioner, with regard to the notification of residents as to when street level images are being taken, the requirement to blur faces and distinguishing information such as licence plate numbers, the length of time that images can be retained, and the procedures to remove images in the case of complaints. In particular, the Committee is assured that the Office of the Privacy Commissioner is, and will continue to monitor developments regarding privacy and street-level imaging to ensure compliance with current Canadian law. For its part, the Committee will also continue to monitor developments in this area and revisit the matter if and when necessary.

However, the emergence of Google's collection of unsecured Wi-Fi payload data raises a broader question about the extent to which privacy concerns are addressed at the development stage of new technologies. As noted by Privacy Commissioner Stoddart, "the

---

90 Ibid. at 1645.

91 Ibid. at 1705.

92 Ibid.

question is, why aren't they starting with privacy principles at the beginning? And why are Canadian taxpayers or Spanish taxpayers and so on spending a lot of time and effort when these companies should get it right from the beginning before they launch their products?"[93]

The Committee is mindful that technology innovators need to ensure that privacy protection is a core consideration at the development stage of any new project. Potential privacy risks should be identified and eliminated or reduced at the onset of new projects and not be left to be addressed as costly afterthoughts. With respect to the specific incident pertaining to Google, the Committee is cautiously optimistic that the company is moving in the right direction by appointing Dr. Alma Whitten as company Director of Privacy, mandating privacy training for its employees, and incorporating more privacy controls, such as audits of projects under development, into the workplace. The Committee looks forward to receiving confirmation that Google has implemented the recommendations made by the Privacy Commissioner in her *Preliminary Letter of Findings* regarding Google's collection of Wi-Fi data by the deadline of February 1, 2011 set by the Privacy Commissioner.

As well, the Committee notes that this study has raised awareness of the importance of privacy protection at Yellow Pages Group, which is now considering how to implement privacy training for employees and consultation with the Privacy Commissioner on product development at Yellow Pages Group.

The Committee commends the Privacy Commissioner of Canada for her work on this file and her work with privacy commissioners internationally on the importance of implementing "privacy by design"[94] into the development of new products in the digital realm.

---

93 Jennifer Stoddart, *Evidence*, Meeting No. 25, October 19, 2010 at 1615, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4702609&Language=E&Mode=1&Parl=40&Ses=3.

94 "Privacy by design" is a concept developed by Ann Cavoukian, PhD, Information and Privacy Commissioner of Ontario, to describe the philosophy of embedding privacy proactively into technology itself—making it the default: http://www.privacybydesign.ca/about/. At the 32nd International Conference of Data Protection and Privacy Commissioners held in Jerusalem, Israel, from October 27-29, 2010, commissioners approved the Privacy by Design Resolution proposed by Dr. Cavoukian and co-sponsored by the Privacy Commissioner of Canada, as well as a number of international privacy commissioners: http://www.ipc.on.ca/english/Resources/News-Releases/News-Releases-Summary/?id=992.

LIST OF RECOMMENDATIONS

RECOMMENDATIONS

1. Given the tremendous changes happening in social media and throughout the Internet, the Committee recommends that the Privacy Commissioner continue to be vigilant in protecting and keeping abreast of the privacy concerns of all Canadians.

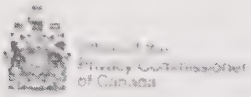
2. The Committee supports the recommendations made by the Privacy Commissioner in her *Preliminary Letter of Findings* regarding Google's collection of Wi-Fi data and calls on Google to implement the Privacy Commissioner's recommendations as soon as possible, and by the deadline of February 1, 2011 as set by the Privacy Commissioner. The Committee recommends that the Privacy Commissioner communicate with the Committee upon receiving confirmation of Google's compliance with her recommendations.

3. The Committee further recommends that the Privacy Commissioner alert the Committee to any concerns that might arise with respect to Google's compliance with her recommendations.

4. The Committee recommends that the Privacy Commissioner clarify with technology providers, such as those seen by the Committee, the importance of having in place explicit privacy training regimes for their employees.

5. The Committee recommends that the Privacy Commissioner continue her outreach activities, such as through the fact sheet prepared for the public titled "*Captured on Camera*—Street-level imaging technology, the Internet and you", to educate the public about their privacy rights and the risks and implications of new technology and social media.

6. Finally, the Committee reiterates the recommendation made by the Privacy Commissioner herself, that technological innovators such as Google should implement "privacy by design" into the development of new products, and consult with the Privacy Commissioner, as well as her international counterparts as appropriate, to ensure that the privacy rights of the public continue to be protected in the digital world.



CAPTURED ON CAMERA
STREET-LEVEL IMAGING TECHNOLOGY, THE INTERNET AND YOU

A number of companies have begun collecting images of public places in Canada, which may then be made available over the Internet or through other means. Individuals may be captured in these images, perhaps incidentally. One of the most widely known is Google's Street View application, which allows computer users to make "virtual visits" to cities such as Paris, London, New York and, eventually, major Canadian centres. Canpages is another company that provides street images on the Internet. Other applications have also been developed for fields such as geomatics, surveying, mapping and urban planning.

In Canada, there is private-sector privacy legislation that applies to these street-level imaging applications if they are collecting images of identifiable people. And, while the Privacy Commissioners of Canada, British Columbia, Alberta and Quebec recognize the popularity of these applications, they have also expressed reservations because the technology captures images not just of places, but of people as well.

The Commissioners believe Canadians should be aware of the privacy issues that can arise.

PEOPLE IN PUBLIC PLACES

A common misconception is that a company doesn't need your permission to take your photograph in a public place.

In fact, one of your key protections under Canadian privacy law is that you should know when your picture is being taken for commercial reasons, and what your image will be used for. Your consent is also needed . There are exceptions to this rule but they are very limited and specific.

However, with some of the new street-level imaging applications, you don't always know if your image is being captured. This is why we think companies that engage in this activity have to let citizens know that they are going to be photographing the streets of their city, when this will happen, why, and how they can have their image removed if they don't want it in a database. For example, this could include visible marking on the vehicles that are used to capture the information, and notification using a variety of media (press release, local media outlets, service web site) outlining dates and locations for filming, the purpose for filming and how people can contact them with questions. Most people

probably don't expect their images to be captured by a company as they go about their business, but they may mind less if they have a choice to plan their day accordingly.

THE PRIVACY DIMENSION AND YOUR IMAGE ONLINE

Street-level imaging applications use various means of photographing the streetscape. Typically, a camera is mounted on a vehicle that is driven up and down the streets of selected cities. The images can then be viewed on the Internet.

Privacy Commissioners have had discussions with several companies to strengthen privacy protections for people whose images are captured. Our position is that all companies that offer such applications must take steps to better safeguard your privacy.

In addition to companies being proactive and creative in their public communications to ensure that Canadians know when their cities -- and, therefore, they themselves -- may be photographed, we think these companies need to be more privacy sensitive in the areas they choose. They need to be mindful that people entering or leaving sensitive locations, such as shelters or abortion clinics, likely want to remain anonymous for privacy and safety reasons.

They should also use proven and effective blurring technologies for faces and vehicle licence plates, so that people cannot be identified when their images are posted. Where individuals may be identifiable, companies must offer fast and responsive mechanisms to allow the images to be blocked or taken down.

Companies offering these imaging applications must also have a good reason to keep the original, unblurred images in their databanks. If they do retain unblurred images, they must limit how long they keep them and protect them with appropriate security measures.

THE BOTTOM LINE

Street-level imaging technology may offer benefits, but these should not come at the cost of your privacy.

That is why we encourage technology companies to ensure that you continue to enjoy your right to privacy, even when you're simply out in the park, walking your dog, or sunning yourself in your backyard.

Federal

Office of the Privacy Commissioner of Canada

Provincial

Information and Privacy Commissioner of Alberta

Information and Privacy Commissioner for British Columbia

Commission d'accès à l'information du Québec

Consent may be express or implied.

In general, under Canadian private-sector privacy legislation, knowledge and consent are not required for journalistic, artistic or literary purposes. There are other exceptions and these can be found in the four applicable private-sector privacy laws: *Personal Information Protection and Electronic Documents Act*; *Personal Information Protection Act* (British Columbia); *Personal Information Protection Act* (Alberta); *La Loi sur la protection des renseignements personnels dans le secteur privé*.

APPENDIX B

PRELIMINARY LETTER OF FINDINGS

Complaints under the Personal Information Protection and Electronic Documents Act (the Act)

1) The Office of the Privacy Commissioner of Canada initiated three complaints against Google Inc. (Google) on May 31, 2010, pursuant to subsection 11(2) of the *Act*, after being made aware that Google Street View cars had been collecting payload data from unencrypted WiFi networks during their collection of publicly broadcast WiFi signals (service set identifiers [SSID] information and Media Access Control ("MAC") addresses.

2) The three complaints are as follows:

   i. Google's collection, use or disclosure of payload data was done without the individual's prior knowledge and consent;

   ii. Google's collection of payload data was done without prior identification of the purposes for which personal information (PI) was collected;

   iii. Google's collection of payload data was not limited to that which was necessary for the purposes identified.

Summary of Investigation

3) Following a request from the German data protection authority in Hamburg to audit the WiFi data collected by Google's Street View cars during a location-based project, Google discovered in May 2010 that it had been collecting payload data from unsecured wireless networks as part of its collection of WiFi data. By Google's own admission, it appears that this inadvertent collection was due to the integration of the code developed in 2006 with the software used to collect WiFi signals. As a result, Google grounded its Street View cars, stopped the collection of WiFi network data on May 7, 2010, and segregated and stored all of the data already collected.

4) On June 1, 2010, our Office sent a letter to Google stating that she was launching an investigation with regard to its collection of payload data. Google responded on June 29, 2010.

5) On June 28, 2010, pursuant to subsection 11(2) of the *Act*, this Office requested to undertake a site visit to Google's facility in Mountain View,

California. The purpose of this site visit was twofold: 1) to allow the review of the payload data gathered by Google, and 2) to ask specific questions of Google's representatives, such as the circumstances surrounding this incident, the segregation and storage of the payload data, and the mitigation and prevention measures Google intended to implement.

6) Google agreed to a site visit. Two technical representatives from this Office then went to the Mountain View facility on July 19, 2010. Although our technicians reviewed the payload data, no Google representatives were available in Mountain View to answer our questions. Instead, by letter dated July 16, 2010, Google answered general questions we posed in a questionnaire we sent on July 12, 2010.

7) On August 18, 2010, a videoconference was held between Google's counsel and this Office in order to answer supplementary questions.

8) The results of our investigation into the three complaints against Google are summarized below in the following sections:

A. Google's Product Counsel's involvement in product review;

B. Circumstances surrounding the collection of payload data and technical testing;

C. Personal information collected;

D. Segregation and storage of the payload data;

E. Google's future plans for its location-based services; and

F. Privacy implications of future plans, and mitigation and prevention measures that Google intends to implement to prevent a recurrence.

A. Google's Product Counsel's involvement in product review

9) Google advised that it has a formal review process for each external product launch. ("External product" denotes a product to be offered to consumers.) This process requires that a Product Counsel assess, among other things, the privacy implications of the product.

10) Since the code ultimately used to sample all categories of publicly broadcast WiFi data is not considered by Google to be an external product, the formal review process did not apply.

11) However, our investigation learned that Google's code design procedure includes a template and process by which the code must be reviewed by Product Counsel before being used or integrated with another Google

product. The template—a methodology document—is in fact mandatory and is the first step in the code design procedure.

12) Our investigation also learned that in the code design-procedure document for the particular code later to be used for the collection of WiFi signals, the engineer did identify one or more privacy concerns about the information collection. These relate to the fact that Google could obtain sufficient data to precisely triangulate a user's position at a given time.

13) The engineer qualified his concerns as being "superficial privacy implications". He did not forward his code design documents to Product Counsel for review—contrary to company procedure. Thus, the code's privacy implications were never assessed.

14) We were also informed that Google's Product Counsel Members consist of practising lawyers with various legal backgrounds. Google claims that they usually have some private-sector experience in privacy issues.

15) According to Google, Product Counsel Members attend the same introductory training session available to all new Google employees. As well, Product Counsel Members participate in weekly privacy- and security-issue meetings. Google also claims that "Privacy is part of the ongoing CLE [Continuing Legal Education] obligations of Google counsel."

B. Circumstances surrounding the collection of payload data and technical testing

16) Google allows its engineers to use 20% of their time to work on projects of interest to them. When using this time in 2006, a Google engineer developed code to sample all categories of publicly broadcast WiFi data.

17) The engineer involved included lines to the code that allowed for the collection of payload data. He thought it might be useful to Google in the future and that this type of collection would be appropriate.

18) This code was later used by Google when it decided to launch a particular location-based service. The service relies on a variety of signals (such as GPS, the location of cell towers and the location of WiFi access points) to provide the user with a location. Google installed antennas and appropriate software (including Kismet, an open-source application) on its Google Street View cars in order to collect publicly broadcast WiFi radio signals within the range of the cars while they travelled through an area. These signals are then processed to identify the WiFi networks (using their MAC address) and to map their approximate location (using the GPS co-ordinates of the car when the signal was received). This information on the identity of WiFi networks and their approximate location then populates the Google location-based services database.

19) In its representations to this Office, Google provided technical information on how it uses WiFi network data for location-based services. Google stated that its software does not store payload transmissions from encrypted networks, but that payload data sent over *unencrypted* WiFi networks is collected and "dumped" on a disk in raw format.

20) However, according to Google, the information thus collected would be fragmented because its cars are on the move when collection occurs and the equipment it uses to collect WiFi signals automatically changes channels five times per second.

21) To our investigation, Google acknowledged that it erred in including in the WiFi-network information-collecting software any code allowing the collection of payload data. Google contends that the code was primarily designed for data-collection software and that this purpose preceded its ultimate application in the collection of WiFi network information for location-based services. Google claims that it did not realize the presence of this code when it began using the software for its geo-location project.

22) It claims that when the decision was made to use the software for collecting publicly broadcast WiFi information, the code was reviewed for bugs and validated by a second engineer before being integrated with, and installed on, Street View cars. The purpose of this review was to ensure the code did not interfere with normal Street View operations. The code was not further examined to verify what kind of data was actually being obtained through the collection of WiFi publicly broadcast signals.

23) Google admitted that since it was not its intention to collect payload data and it never intended to use payload data in any of its products, it was not in a position to identify any purposes for the collection of these data or seek consent from affected individuals. Google also admitted that it did not inform any affected individuals of the fact that it was collecting payload data since its employees did not realize they were doing so until May 2010.

24) Google provided three reasons to explain why the collection of payload data was not discovered earlier:

    i. No one other than the engineer who developed the code was interested in looking at this program. No one thought payload data would be useful and no one had planned to use this data.

    ii. Payload data comprised a minuscule amount of the total data collected. Its collection was thus of minimal concern and no one had any reason to examine it.

iii. The engineer had not seen the ramifications of including this code and, consequently, had not spoken of it with his manager.

25) Google also asserted that since it had no purpose for the collection of payload data, there cannot be any justification for its retention. Consequently, Google is anticipating its secure destruction as soon as possible and is seeking this Office's authorization to do so.

26) Our investigation revealed that Google collected WiFi data in Canada from March 30, 2009 to May 7, 2010, and that its Street View cars have driven most urban areas and major roads.

27) Google stated that it cannot accurately distinguish between WiFi networks and wireless devices. It can, however, identify the unique number of basic service set identifiers (a.k.a. BSSIDs), which generally identify a single WiFi access point. Although the BSSID does identify an access point, it does not indicate how many devices or networks connect through the access point.

28) Google estimates that it collected over 6 million BSSIDs over the period its Street View cars drove throughout Canada.

C. Personal information collected

29) Our two technical experts visited Google's offices in Mountain View, California on July 19 and 20, 2010. The purpose of this site visit was for them to examine the data that had been collected by Google's Street View cars for Google's location-based services so as to determine its nature and the quantity involved. Their examination focussed on finding examples of personal information within the WiFi payload data collected in Canada.

30) Our technical experts searched the payload data to find anything that could constitute personal information (e.g., examples of e-mail, usernames, passwords and phone numbers). They produced an approximate count of possible personal information through an automated search. For example, the count included 787 e-mail headers and 678 phone numbers. However, a match does not mean a perfect identification. The searches may have included irrelevant items, or missed some items.

31) To complement the automated search, our experts performed a manual verification for five instances of each type of personal information. This was to demonstrate the existence of each data type, while preventing our experts from intruding too deeply into any individual's personal information.

32) Our technical experts found at least five instances of e-mails where they noted the presence of e-mail addresses, complete e-mail headers, IP addresses, machine hostnames, and contents of messages. The messages were truncated in the five instances of e-mails they found, but when performing a manual verification for other items (e.g., phone numbers), they observed complete e-mail messages.

33) They also found five instances of usernames. These could be seen in cookies, MSN messages and chat sessions. They also found one instance where a password and username were included in an e-mail message that a person was sharing with others to tell them how to log in to a server.

34) Our experts also found at least five instances of real names of individuals, five instances of residential addresses and five more of business addresses. They noted that, unlike the residential addresses, the business addresses were very common.

35) They also found five instances of instant messenger headers and five instances of phone numbers—both business and personal phone numbers. Like business addresses, business phone numbers were easier to find than personal ones.

36) A search for nine-digit or sixteen-digit numbers, which could have been Social Insurance Numbers (SIN) or credit card numbers, did not turn up anything due to there being too many other instances of irrelevant or similar numbers in the dataset. Therefore, although we found no evidence of SIN or credit cards numbers being collected, we still cannot entirely rule out the possibility that they were.

37) Our technical experts also noticed sensitive items during their searches. For example, they found a list of names, phone numbers, addresses and medical conditions for specified individuals. They also found a reference to someone stopped for a speeding violation, along with address information.

38) Our experts often saw cookies being passed from client machines to Web servers. These cookies were unencrypted and some contained personal information, including IP addresses, user names and postal addresses. They were surprised by the frequency of unencrypted cookies containing personal information.

39) In summary, our experts found many instances of personal information in the sample they took of the payload data collected in Canada by Google.

D. Segregation and the storage of the payload data

40) The WiFi data was collected through WiFi antennas attached to the roof of Street View cars. This WiFi antenna passively received the publicly

broadcast radio signals within range of the car using open-source Kismet software. The data was then relayed to a Google-developed application called "gStumbler" and its executable program "gslite", which processed the data for storage. The data was then saved to hard drives physically located in each Street View car and then subsequently transferred to Google's servers.

41) Google alleges it grounded its Street View cars and segregated the payload data on a restricted area of its network as soon as it became aware that its gStumbler application was collecting payload data from unencrypted WiFi networks.

42) As a follow up step, a Google system administrator copied onto a total of four disks the files containing the payload data collected in all affected countries. This was done from May 9, 2010, to May 13, 2010. These disks contained two copies of the data: one copy obtained after categorizing and labelling the data files by country, and one copy of the data before categorizing.

43) On May 15, 2010, the system administrator consolidated the payload data onto an encrypted hard drive, segregated by country. A second copy of the encrypted hard drive was made for security and backup preservation. The four original disks were then destroyed in a disk deformer.

44) A Google employee personally delivered one encrypted hard drive to another Google location for safekeeping, while the system administrator kept the other one in a secure location. Once the Google employee arrived at the destination, the system administrator permanently destroyed the backup, encrypted hard drive. The US data was then segregated onto a separate encrypted drive, while the data from the rest of the world remained on the initial encrypted drive.

E. Google's future plans for its location-based services

45) Google still intends to offer location-based services, but does not intend to resume collection of WiFi data through its Street View cars. Collection is discontinued and Google has no plans to resume it.

46) Google does not intend to contract out to a third party the collection of WiFi data.

47) Google intends to rely on its users' handsets to collect the information on the location of WiFi networks that it needs for its location-based services database. The improvements in smart-phone technology in the past few years have allowed Google to obtain the data it needs for this purpose from the handsets themselves.

48) Although it has no tracking tool to keep records of a customer's locations (and does not intend to create one), Google acknowledges that it does need to examine the potential privacy concerns of this method of collection.

F. Privacy implications of future plans, and mitigation and prevention measures

49) Google submits that it is striving to design privacy protections into all its products and services. It states that its employees receive orientation and code-of-conduct training that includes a privacy and data-security component. However, the responsibility of aligning Google's projects with its Privacy Principles and Privacy Policy lies with each of its product and engineering teams.

50) Google also states that as products are chartered or otherwise provided with resources and staffing, they are assigned to a Product Counsel in Google's legal department. This individual has a first-level responsibility for identifying privacy issues in a product.

51) In order to avoid a recurrence of a product design having a negative impact on privacy, Google claimed to be reviewing its product launch procedures, code review procedures and 20% time policy. In so doing, it would ensure that its internal controls are robust enough to adequately address future issues. As of the issue date of this report, Google's review of its procedures/policies has not yet been completed.

Application

52) In making our determinations, we applied Principles 4.1.1 and 4.1.2 of the *Personal Information Protection and Electronic Documents Act*. Principle 4.1.1 stipulates that accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s). Principle 4.1.2 continues that the identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

53) We also applied Principle 4.2, which states that the purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

54) Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate

55) Lastly, Principle 4.4 states that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.

Findings

56) On September 15, 2010, I shared an earlier version of this report with Google and invited their response. Taking into consideration their response, I have revised my preliminary letter of findings. What follows is a summary of our findings and recommendations.

Collection of personal information

57) During their site visit, our technical experts uncovered substantial amounts of personal information in the form of e-mail message content (e.g., e-mail, IP and postal addresses), captured in Google's collection of payload data in Canada.

58) Google acknowledged to this Office that it did collect payload data, but not with the intent of using it in any of its products. According to Google, it was "simply mistaken" in collecting the data and did not seek consent from the affected individuals. Principle 4.3 of the *Act* requires that the knowledge and consent of the individual be obtained for the collection, use or disclosure of their personal information.

59) Google also stated that it had not identified any purposes for the collection of the payload data. Principle 4.2 requires that such a purpose be identified at or before the time of collection. Further, Principle 4.4 stipulates that the collection of personal information be limited to that which is necessary for the purposes identified. Since no purpose could be identified, it follows that the collection in this case clearly could not be limited to any specific purpose. This is in violation of Principle. 4.4.

Google's Product Counsel's involvement

60) Due to the engineer's failure to forward his design document to the Product Counsel, the Counsel was unable to assess the privacy implications of the code designed to collect WiFi data. This is a careless error that I take very seriously since a review of design documents by a Product Counsel (and the use of a template) is clearly a mandatory step in Google's code design procedure.

61) As a result, the un-scrutinized code was later used to collect data containing personal information. If the Product Counsel had been involved when and as it should have been, Google may have discovered the risk of data over-collection and would have been in a position to remedy the situation before any collection took place. The ensuing negative effects on citizens' privacy and Google's reputation could easily have been avoided.

62) Google informed our Office that engineering and product teams are accountable for complying with Google's privacy policies and principles. Google then stated that it is working towards improving its code-and-product review processes, as well as accountability mechanisms, for engineering and product management personnel in order to improve their sensitivity to privacy issues at all stages of product and code development. A legal team is working with engineering directors to ensure a comprehensive review of codes for any privacy issues. Google believes that the review of its policies and procedures that it has undertaken will ensure no recurrences. Google stated that it will keep this Office informed as Google completes its review.

Code review and testing

63) Google asserted that the engineer who developed the lines of code did not see its ramifications of ultimately allowing the collection of a broader range of data from wireless networks. Our investigation was not able to determine with certainty if this was a one-time error committed by one individual or, perhaps, a sign of a more generalized lack of awareness among employees with regards to privacy implications of new products. At Google, the effects of new products on privacy should be well understood not only by the Product Counsel but also by the professionals who develop these products.

64) In this case, the review and testing of the product containing the code were insufficient to assess privacy impact. It would appear that the review consisted merely of ensuring that the product did not interfere with a second application—that used to collect pictures of the streets navigated by Street View vehicles.

65) As our investigation revealed, the review was not able to assess the extended capabilities of the product—including its ability to collect more information than necessary for the location-based project.

Steps taken to protect payload data

66) Once Google realized its Street View cars were collecting more data from wireless networks than anticipated, Google expressed regret in inadvertently collecting the publicly broadcast data. It immediately

grounded its vehicles and took measures to safeguard the collected payload data and segregate it by country of origin.

67) Google's actions were justified, appropriate and sufficient to safeguard the payload data collected in Canada. In my view, Google upheld the related safeguard provisions under the *Act*.

68) Concerning the data that Google collected, it affirmed that it has no desire to use the Canadian payload data in any manner and will continue to secure the data with strenuous access restrictions until it is deleted.

69) To this, I would like to add that not only privacy laws, but other applicable laws in the U.S. and in Canada, including laws of evidence, must also be taken into account in determining when to delete the Canadian payload data collected.

Future plans

70) The fact that Google does not intend to resume collection of WiFi data with its Street View cars eliminates the possibility of further inappropriate collection of personal information through the tool developed by its engineer.

71) However, from users' handsets, Google intends to obtain the information needed to populate its location-based services database. This alternative method of collection could also lead to inappropriate collection and retention of personal information if Google does not put in place appropriate safeguard measures.

Recommendations

72) I share Google's goal to avoid recurrences of any similar violations of individuals' privacy. While I am pleased that Google has taken under review its processes and procedures that could impact privacy, I would nonetheless like the organization to ensure that these controls are complemented by an overarching governance model embodying all privacy issues pertaining to the design of internal/external products and services. I would also like Google to respect reasonable timelines to implement both the governance model and the revised processes and procedures. With this view, and after reviewing the additional information Google provided this Office, I am making the following recommendations:

i. That Google re-examine and improve the privacy training it provides all its employees, with the goal of increasing staff awareness and understanding of Google's obligations under privacy laws.

ii. That Google ensure it has a governance model in place that includes:

- effective controls to ensure that all necessary procedures to protect privacy have been duly followed prior to the launch of any product;
- clearly designated and identified individuals actively involved in the process and accountable for compliance with Google's obligations under privacy laws.

iii. That Google delete the Canadian payload data it collected, to the extent that Google is allowed to do so under Canadian and U.S. laws. If the Canadian payload data cannot immediately be deleted, the data needs to be properly safeguarded and access thereto is to be restricted.

73) At this time, I consider the matter to be **well-founded** and still **unresolved**. My Office will only consider the matter resolved upon receiving either by or before February 1, 2011, confirmation of the implementation of the above recommendations, at which point I will issue my final report and conclusions.

APPENDIX C

LIST OF WITNESSES
SECOND SESSION, 40TH PARLIAMENT

Organizations and Individuals	Date	Meeting
Canpages Inc.	2009/06/17	29
Olivier Vincent, President and Chief Executive Officer		
Google Inc.		
Jonathan Lister, Managing Director and Head of Google Canada		
Office of the Privacy Commissioner of Canada	2009/10/22	32
Carman Baggaley, Strategic Policy Advisor		
Daniel Caron, Legal Counsel, Legal Services, Policy and Parliamentary Affairs Branch		
Elizabeth Denham, Assistant Privacy Commissioner		

THIRD SESSION, 40TH PARLIAMENT

Organizations and Individuals	Date	Meeting
Office of the Privacy Commissioner of Canada	2010/10/28	28
Daniel Caron, Legal Counsel, Legal Services, Policy and Parliamentary Affairs Branch		
Patricia Kosseim, General Counsel		
Andrew Patrick, Information Technology Research Analyst		
Google Inc.	2010/11/04	30
Jacob Glick, Canada Policy Counsel		
Google Inc.	2010/11/25	34
Jacob Glick, Canada Policy Counsel		
Alma Whitten, Engineering Lead for Privacy		
Yellow Pages Group Co.		
Martin Aubut, Senior Manager, Social Commerce		
François D. Ramsay, Senior Vice-President, General Counsel, Secretary and Responsible for Privacy		

APPENDIX D

LIST OF BRIEFS
SECOND SESSION, 40TH PARLIAMENT

Organizations and individuals
Google Inc.

MINUTES OF PROCEEDINGS

A copy of the relevant Minutes of Proceedings (40th Parliament, 3rd Session: Meetings Nos. 28, 30, 32, 34, 37 and 39) and (40th Parliament, 2nd Session: Meetings Nos. 29 and 32) is tabled.

Respectfully submitted,

Hon. Shawn Murphy, P.C., MP
Chair

PROCÈS-VERBAUX

Un exemplaire des procès-verbaux pertinents (40e législature, 3e session : séances nos 28, 30, 32, 34, 37 et 39) et (40e législature 2e session : séances nos 29 et 32) est déposé.

Respectueusement soumis,

Le président,

L'hon. Shawn Murphy, C.P., député

ANNEXE D

LISTE DES MÉMOIRES
DEUXIÈME SESSION, 40E LÉGISLATURE

Organisations et individus

Google inc.

Groupe Pages Jaunes Cie

Martin Aubut, premier directeur,
Commerce social

François D. Ramsay, premier vice-président, conseiller juridique principal, secrétaire et responsable du respect de la vie privée

ANNEXE C

LISTE DES TÉMOINS
DEUXIÈME SESSION, 40e LÉGISLATURE

Organisations et individus	Date	Réunion
Canpages inc.	2009/06/17	29
Olivier Vincent, président et chef de direction		
Google inc.		
Jonathan Lister, directeur général et chef de Google Canada		
Commissariat à la protection de la vie privée du Canada	2009/10/22	32
Carman Baggaley, conseiller en politiques stratégiques		
Daniel Caron, conseiller juridique, Direction des services juridiques, des politiques et des affaires parlementaires		
Elizabeth Denham, commissaire adjointe à la protection de la vie privée		

TROISIÈME SESSION, 40e LÉGISLATURE

Organisations et individus	Date	Réunion
Commissariat à la protection de la vie privée du Canada	2010/10/28	28
Daniel Caron, conseiller juridique, Direction des services juridiques, des politiques et des affaires parlementaires		
Patricia Kosseim, avocate générale		
Andrew Patrick, analyste de recherche en technologie de l'information		
Google inc.	2010/11/04	30
Jacob Glick, conseiller en matière de politique au Canada		
Google inc.	2010/11/25	34
Jacob Glick, conseiller en matière de politique au Canada		
Alma Whitten, chef technique à la protection de la vie privée		

i. Que Google réexamine et améliore la formation offerte à tous les employés au sujet du respect de la vie privée, dans le but d'améliorer la conscientisation et la connaissance des employés quant aux obligations de Google en vertu des lois sur la protection des renseignements personnels.

ii. Que Google instaure un modèle de gouvernance qui comprenne :

- des mesures de contrôle efficaces visant à faire en sorte que toutes les procédures nécessaires au respect de la vie privée ont bel et bien été suivies avant le lancement de tout produit;

- la désignation et l'identification claires de personnes responsables du respect des obligations de Google en vertu des lois sur la protection des renseignements personnels.

iii. Que Google supprime les données utiles canadiennes recueillies, dans la mesure où elle est habilitée à le faire aux termes des lois canadiennes et américaines. Si les données utiles canadiennes ne pouvaient pas être supprimes sur le champ, elles devraient être conservées de manière sécuritaire et l'accès à ces données devrait être restreint.

73) À l'heure actuelle, j'estime que la plainte est **fondée** et demeure **non résolue.** Le Commissariat ne considérera l'affaire résolue que si Google lui remet au plus tard le 1er février 2011 la confirmation que les recommandations formulées ci-dessus ont été mises en œuvre; j'émettrai à ce moment mes conclusions et mon rapport finaux.

67) La démarche de Google était justifiée, appropriée et suffisante pour protéger les données utiles recueillies au Canada. Je crois que l'entreprise a respecté les clauses pertinentes de la *Loi*.

68) Pour ce qui est des données que Google a recueillies, l'entreprise a affirmé qu'elle n'avait aucunement l'intention d'utiliser les données utiles canadiennes de quelque façon que ce soit, et qu'elle continuera de garder les données en toute sécurité et d'en restreindre activement l'accès d'ici à ce que ces données soient supprimées.

69) Je tiens à ajouter ici que l'on doit tenir compte non seulement des lois sur la protection des renseignements personnels, mais aussi d'autres lois canadiennes et américaines, y compris les règles de droit sur la preuve, afin de déterminer le moment opportun pour supprimer les données utiles canadiennes recueillies.

Plans d'avenir

70) Le fait que Google n'a pas l'intention de reprendre la collecte de données Wi-Fi à l'aide de ses voitures Street View élimine le risque d'une nouvelle collecte de renseignements personnels inappropriée au moyen de l'outil conçu par l'ingénieur.

71) Cependant, Google prévoit recueillir des renseignements à partir des appareils portables des utilisateurs pour alimenter sa base de données sur les services géodépendants. Cette nouvelle méthode pourrait aussi mener à la collecte et à la conservation inappropriées de renseignements personnels si Google ne prenait pas les mesures de protection qui s'imposent.

Recommandations

72) Je partage l'objectif de Google visant à éviter que des atteintes similaires à la vie privée des personnes se reproduisent. Bien que je sois heureuse de constater que Google a entrepris l'examen des processus et des procédures pouvant avoir une incidence sur la protection de la vie privée, je souhaite néanmoins que l'organisation complète ces mesures de contrôle par un modèle de gouvernance global qui tient compte de toutes les questions liées à la protection de la vie privée associées à la conception de produits et de services internes et externes. J'aimerais également que Google respecte des échéanciers raisonnables pour la mise en œuvre tant du modèle de gouvernance que des procédures et des processus révisés. C'est dans cette optique et à la lumière des renseignements supplémentaires que Google a présentés au Commissariat que j'émets les recommandations suivantes :

62) Google a indiqué au Commissariat qu'il incombe aux équipes de l'ingénierie et de l'élaboration de produits de respecter les politiques et les principes en matière de protection de la vie privée de l'entreprise. Google a ensuite déclaré qu'elle déploie des efforts en vue d'améliorer les processus d'examen des codes et des produits, ainsi que les mécanismes de responsabilisation, que doivent suivre le personnel de l'ingénierie et de la gestion de produits afin de les sensibiliser davantage aux enjeux de vie privée à toutes les étapes d'élaboration de produits et de codes. Une équipe juridique travaille avec les directeurs de l'ingénierie pour s'assurer qu'un examen exhaustif des codes est effectué afin de déterminer si ces derniers pourraient soulever des questions liées à la vie privée. Google estime que l'examen des politiques et des procédures qu'elle a entrepris fera en sorte que la situation ne se reproduira plus. Google a déclaré qu'elle tiendra le Commissariat au courant de la progression de l'examen.

Examen et essai du code

63) Google soutient que l'ingénieur qui a élaboré les lignes de code ne se doutait pas que leur utilisation aboutirait à la collecte d'une vaste gamme de données transmises par des réseaux sans fil. Notre enquête n'a pas permis de déterminer s'il s'agissait d'une erreur ponctuelle d'une seule personne ou si c'était le signe que les employés en général ne sont pas suffisamment sensibilisés aux répercussions des nouveaux produits sur la vie privée. Chez Google, ces conséquences devraient être bien comprises par les conseillers juridiques en matière de produits, mais aussi par les professionnels qui mettent au point ces produits.

64) Dans le présent cas, l'examen et l'essai du produit contenant le code n'ont pas permis d'évaluer l'incidence sur la vie privée. Il semble que l'examen visait seulement à s'assurer que le produit ne nuirait pas à une deuxième application — celle qui a servi à prendre des images des rues où circulaient les véhicules Street View.

65) Notre enquête a démontré que l'examen n'a pas suffi à évaluer toutes les capacités du produit — y compris celle de recueillir des données qui ne sont pas nécessaires au projet de géolocalisation.

Mesures prises pour protéger les données utiles

66) Lorsque Google a remarqué que ses voitures Street View recueillaient plus de données transmises par les réseaux sans fil que prévu, elle a exprimé du regret quant à la collecte par inadvertance des données diffusées publiquement. Elle a immédiatement immobilisé ses véhicules et pris des mesures pour protéger les données utiles et les isoler par pays d'origine.

présente lettre de conclusions préliminaire en tenant compte de la réponse de Google. Les paragraphes qui suivent sont un résumé de nos conclusions et de nos recommandations.

Collecte de renseignements personnels

57) Au cours de leur visite sur les lieux, nos spécialistes ont découvert une quantité substantielle de renseignements personnels sous la forme de contenu de courriels (p. ex des adresses courriel, IP et postales) parmi les données utiles recueillies par Google au Canada.

58) Google a avoué au Commissariat qu'elle avait recueilli des données utiles, mais sans avoir l'intention de les utiliser dans l'un ou l'autre de ses produits. Elle affirme avoir tout simplement recueilli les données par erreur et n'a pas demandé le consentement des personnes touchées. Le principe 4.3 de la *Loi* exige que la personne concernée consente à la collecte, à l'utilisation et à la communication de renseignements personnels.

59) Google déclare aussi que la collecte de données utiles n'avait aucun objectif. Or, le principe 4.2 stipule que l'objectif doit être établi avant la collecte ou au moment de celle-ci. En outre, le principe 4.4 précise que seuls les renseignements personnels nécessaires aux fins déterminées doivent être recueillis. Étant donné qu'aucune fin n'a été établie, la collecte de données ne pouvait évidemment pas être limitée par un objectif précis, ce qui est contraire au principe 4.4.

La participation du conseiller juridique en matière de produits de Google à l'examen des produits

60) Puisque l'ingénieur a omis de transférer son document de conception au conseiller juridique en matière de produits, ce dernier n'a pas pu évaluer les répercussions sur la vie privée du code visant à recueillir les données Wi-Fi. Je considère que cette négligence est très grave puisque l'examen des documents de conception par un conseiller juridique en matière de produits (et l'utilisation d'un modèle) est manifestement une étape obligatoire prévue dans la procédure d'élaboration de code de Google.

61) Le code non étudié a plus tard servi à recueillir des données comprenant des renseignements personnels. Si le conseiller juridique en matière de produits avait été mis à contribution comme il aurait dû l'être, Google aurait peut-être découvert le risque d'une collecte excessive et remédié à la situation avant que des données ne soient recueillies. Les répercussions négatives sur la vie privée des citoyens et sur la réputation de Google auraient facilement pu être évitées.

de la vie privée incombe à toutes les équipes de production et de conception.

50) Google soutient également que, lorsque les produits sont approuvés ou que les ressources et le personnel leur sont attribués, ils sont confiés à un conseiller juridique en matière de produits de l'entreprise. Il a une responsabilité de premier niveau pour ce qui est de cerner les préoccupations liées à la protection de la vie privée liées à un produit.

51) Pour éviter qu'un autre produit ait des répercussions néfastes sur la vie privée, Google dit examiner ses procédures liées au lancement de produits et à l'examen de code, ainsi que sa politique qui consiste à laisser ses employés décider de 20 % de leur emploi du temps. Ces mesures feraient en sorte que les contrôles internes seraient suffisamment efficaces pour aborder adéquatement les futurs enjeux. Au moment de la diffusion du présent rapport, l'examen de Google sur ses politiques et procédures n'était pas encore terminé.

Application

52) Pour en arriver à nos conclusions, nous avons appliqué les principes 4.1.1 et 4.1.2 de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Selon le principe 4.1.1, il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes, même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidien des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées. Selon le principe 4.1.2, il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.

53) Nous avons également appliqué le principe 4.2, qui précise que les fins pour lesquelles les renseignements personnels sont recueillis doivent être établies par l'organisation avant ou pendant la collecte.

54) Le principe 4.3 stipule que toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

55) Enfin, le principe 4.4 indique que l'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées par l'organisation.

Conclusions

56) Le 15 septembre 2010, j'ai transmis à Google une version préalable du présent rapport et invité l'organisme à formuler une réponse. J'ai révisé la

43) Le 15 mai 2010, l'administrateur système a réuni les données utiles sur un disque dur crypté et les a divisées par pays. Une copie de sauvegarde du disque dur crypté a été enregistrée. Les quatre premiers disques ont été détruits dans un outil de déformation physique.

44) Un employé de Google a livré en main propre un disque dur crypté à un autre bureau de l'entreprise aux fins de sauvegarde; l'administrateur système a conservé l'autre disque en lieu sûr. Lorsque l'employé de Google est arrivé à destination, l'administrateur système a détruit définitivement le disque dur crypté de sauvegarde. Les données américaines ont été isolées sur un disque crypté distinct alors que les données du reste du monde sont demeurées sur le disque crypté d'origine.

E. Les plans d'avenir de Google concernant ses services géodépendants

45) Google a toujours l'intention d'offrir des services géodépendants, mais ne prévoit pas reprendre la collecte de données Wi-Fi au moyen de voitures Street View. Cette collecte est interrompue et Google ne prévoit pas la reprendre.

46) Google n'a pas l'intention d'impartir à une tierce partie la cueillette des données Wi-Fi.

47) L'entreprise pense plutôt se servir des appareils portables de ses utilisateurs pour recueillir les renseignements sur l'emplacement des réseaux Wi-Fi dont elle a besoin pour sa base de données sur les services géodépendants. L'amélioration des téléphones intelligents au cours des dernières années a permis à Google de recueillir les données requises à cette fin à partir des appareils portables eux-mêmes.

48) Bien qu'elle ne dispose d'aucun outil pour faire le suivi des déplacements d'un consommateur (et elle n'a pas l'intention d'en créer un), Google convient qu'elle doit examiner les problèmes que pourrait poser cette méthode de collecte relativement à la vie privée.

F. Les répercussions des plans d'avenir sur la protection de la vie privée et les mesures d'atténuation et de prévention

49) Google fait valoir qu'elle tente d'intégrer des mesures de protection des renseignements personnels dans tous ses produits et services. Elle affirme que ses employés reçoivent une séance de formation initiale et une formation sur le code de déontologie qui comprennent une partie sur la protection des renseignements personnels et la sécurité des données. Cependant, la responsabilité d'harmoniser tous les projets de Google avec les principes et les politiques de l'entreprise en matière de protection

36) Les recherches de numéros à 9 ou à 16 chiffres, qui auraient pu être des numéros d'assurance sociale (NAS) ou de carte de crédit, n'ont donné aucun résultat puisqu'il y avait trop de numéros non pertinents ou semblables dans l'ensemble des données. Par conséquent, bien que nous n'ayons pas trouvé la preuve que des numéros d'assurance sociale ou de carte de crédit étaient recueillis, la possibilité ne peut être exclue.

37) Nos spécialistes ont aussi découvert des éléments sensibles, comme une liste de noms, de numéros de téléphone, d'adresses et de problèmes de santé liés à des personnes précises. Ils ont aussi trouvé une allusion à une personne arrêtée pour excès de vitesse, avec son adresse.

38) Les spécialistes ont vu de nombreux témoins transmis par des ordinateurs clients à des serveurs Web. Ces témoins n'étaient pas cryptés et certains d'entre eux comprenaient des renseignements personnels comme des adresses IP, des noms d'utilisateur et des adresses postales. Les enquêteurs ont été surpris du nombre de témoins non cryptés qui comprenaient des renseignements personnels.

39) Bref, nos spécialistes ont trouvé de nombreux renseignements personnels dans l'échantillon prélevé des données utiles recueillies au Canada par Google.

D. L'isolement et le stockage des données utiles

40) Les données Wi-Fi ont été captées au moyen d'antennes installées sur le toit des voitures Street View. Cette antenne recevait passivement les signaux radio publics à portée de la voiture à l'aide du logiciel libre Kismet. Les données étaient ensuite transmises à l'application « gStumbler », créée par Google, et à son programme exécutable « gslite », qui traitait les données en vue du stockage. Les données étaient ensuite enregistrées sur des disques durs physiques placés dans chaque voiture Street View, puis transférées sur les serveurs de Google.

41) Google affirme avoir interrompu les activités de ses voitures Street View et isolé les données utiles dans une zone d'accès restreint de son réseau dès qu'elle a pris conscience que l'application gStumbler recueillait les données utiles des réseaux Wi-Fi non cryptés.

42) Par la suite, un administrateur système de Google a copié sur un total de quatre disques les fichiers comprenant les données utiles recueillies dans tous les pays touchés. Cette opération s'est déroulée du 9 au 13 mai 2010. Les disques contenaient deux copies des données : la première a été obtenue après le classement par catégorie et l'étiquetage des dossiers de données par pays, et la seconde, avant le classement des données.

C. La collecte de renseignements personnels

29) Les deux spécialistes du Commissariat ont visité les bureaux de Google à Mountain View (Californie) les 19 et 20 juillet 2010. L'objectif de cette visite était d'examiner les données recueillies pour les services géodépendants par les voitures de Google Street View afin d'en déterminer la nature et la quantité. L'examen visait principalement à trouver des exemples de renseignements personnels dans les données utiles tirées des réseaux Wi-Fi du Canada.

30) Nos spécialistes ont effectué des recherches dans les données utiles pour trouver tout ce qui pourrait constituer un renseignement personnel (p. ex. des courriels, des noms d'utilisateur, des mots de passe et des numéros de téléphone). Ils ont fait un décompte approximatif des renseignements personnels au moyen d'une recherche automatisée. Pour donner un ordre de grandeur, le décompte comprenait 787 en-têtes de courriel et 678 numéros de téléphone. Cependant, ces recherches peuvent comprendre des résultats non pertinents ou passer outre certains éléments.

31) Pour compléter la recherche automatisée, nos spécialistes ont vérifié manuellement cinq occurrences de chaque type de renseignement personnel. L'objectif était de prouver l'existence de chacun de ces types de données sans envahir indûment la vie privée des personnes concernées.

32) Nos spécialistes ont découvert au moins cinq courriels dont ils ont vu les adresses, les en-têtes complets, les adresses IP, les noms d'hôte des appareils et le contenu des messages. Les cinq messages étaient tronqués, mais les spécialistes ont trouvé des courriels complets en vérifiant manuellement d'autres éléments (comme des numéros de téléphone).

33) Cinq noms d'utilisateur ont aussi été découverts. Ils se trouvaient dans les témoins de connexion, les messages transmis par MSN et les séances de clavardage. Les spécialistes ont aussi trouvé un cas où un mot de passe et un mot d'utilisateur étaient compris dans un courriel destiné à expliquer à des gens comment se connecter à un serveur.

34) Nos spécialistes ont aussi trouvé cinq noms de personnes véritables, cinq adresses résidentielles et cinq autres adresses d'entreprises. Ils ont remarqué que, contrairement aux adresses résidentielles, les adresses d'entreprises étaient très répandues.

35) Ils ont aussi trouvé cinq messages instantanés et cinq numéros de téléphone -tant d'entreprises et que de résidences. Tout comme les adresses, les numéros de téléphone des entreprises étaient plus faciles à trouver que les numéros personnels.

genre de données obtenues au moyen de la réception de signaux publics sur des réseaux Wi-Fi.

23) Google a admis que, puisqu'elle n'avait pas l'intention de recueillir des données utiles et qu'elle n'a jamais voulu inclure de telles données dans l'un ou l'autre de ses produits, elle ne pouvait ni indiquer la fin de la collecte ni obtenir le consentement des personnes touchées. Elle a également avoué qu'elle n'avait pas avisé les personnes concernées par la collecte de données utiles puisque les employés n'étaient pas conscients qu'ils en avaient recueillies avant mai 2010.

24) Google a invoqué trois raisons expliquant pourquoi la collecte de données utiles n'a pas été découverte plus tôt:

i. Hormis l'ingénieur qui a élaboré le code, aucun employé n'était intéressé à examiner ce programme : personne ne croyait que les données utiles pourraient servir et personne n'avait l'intention d'utiliser ces données.

ii. Étant donné que les données utiles formaient une infime partie de l'ensemble des données recueillies, leur collecte n'était guère préoccupante et il n'y avait aucune raison de les examiner.

iii. L'ingénieur n'a pas anticipé les conséquences de l'inclusion de ce code et n'a donc pas abordé la question avec son gestionnaire.

25) Google a aussi affirmé que, puisque la collecte de données utiles ne présente aucun intérêt, rien ne justifie de les conserver. Par conséquent, Google prévoit les détruire de façon sécuritaire aussitôt que possible, et elle demande l'autorisation du Commissariat pour s'exécuter.

26) Notre enquête a révélé que Google a recueilli des données Wi-Fi au Canada du 30 mars 2009 au 7 mai 2010 et que les voitures Street View ont sillonné la plupart des régions urbaines et des routes principales.

27) Google souligne qu'elle ne peut distinguer précisément les réseaux Wi-Fi des appareils sans fil. Elle peut toutefois cerner le numéro unique des identificateurs d'ensemble de services de base (IDESB), qui identifient généralement un point d'accès Wi-Fi unique. Les IDESB permettent d'identifier un point d'accès, mais ils n'indiquent pas combien d'appareils ou de réseaux s'y connectent.

28) Google estime avoir recueilli plus de 6 millions d'IDESB pendant que ses voitures Street View parcouraient le Canada.

17) L'ingénieur en question a ajouté des lignes de code permettant de recueillir des données utiles. Il a pensé que cela pourrait éventuellement servir à Google et qu'une telle collecte serait appropriée.

18) Google a utilisé ce code lorsqu'elle a décidé de lancer un certain service géodépendant qui se basait sur divers signaux (comme les GPS et l'emplacement de stations de base et de points d'accès Wi-Fi) pour indiquer un endroit à un utilisateur. Elle a installé des antennes et les logiciels requis (dont Kismet, une application libre) à bord de ses voitures Street View afin de capter les signaux Wi-Fi publics à portée de ces véhicules pendant que ceux-ci circulent dans un quartier. Les signaux étaient ensuite traités pour identifier les réseaux Wi-Fi (à l'aide de leur adresse MAC) et cerner leur emplacement approximatif (à l'aide des coordonnées fournies par le GPS au moment où le signal était reçu). Les renseignements sur l'identité des réseaux Wi-Fi et leur emplacement approximatif alimentent ensuite la base de données des services géodépendants de Google.

19) Dans ses observations présentées au Commissariat, Google a fourni des renseignements techniques sur sa façon d'utiliser les données transmises par les réseaux Wi-Fi pour les services géodépendants. Elle a mentionné que son logiciel n'enregistre pas les données utiles transmises par des réseaux cryptés, mais que les données utiles diffusées sur des réseaux Wi-Fi non cryptés sont recueillies et enregistrées sur un disque en format brut.

20) Toutefois, selon Google, les renseignements ainsi recueillis seraient fragmentés puisque les voitures sont en mouvement au moment de la collecte et que l'équipement servant à recueillir les signaux Wi-Fi automatiquement change de fréquence cinq fois par seconde.

21) Au cours de notre enquête, Google a reconnu avoir erré en insérant un code permettant de recueillir des données utiles dans le logiciel de collecte de renseignement sur les réseaux Wi-Fi. Elle soutient que le code a surtout été conçu pour un logiciel de collecte de données, et que cet objectif avait préséance sur son utilisation ultime dans le cadre de la collecte de renseignements sur les réseaux Wi-Fi pour des services géodépendants. Google affirme qu'elle n'était pas consciente de la présence de ce code lorsqu'elle a commencé à utiliser le logiciel pour son projet de géolocalisation.

22) Selon Google, quand l'entreprise a décidé d'utiliser le logiciel pour recueillir des renseignements publics sur les réseaux Wi-Fi, le code a été examiné pour découvrir les bogues, puis validé par un deuxième ingénieur avant d'être installé à bord des voitures Street View. Cette opération visait à s'assurer que le code ne nuirait pas aux opérations habituelles de Street View. Aucune vérification approfondie n'a été effectuée pour vérifier le

10) Google considère que le code qui a finalement servi à relever toutes les catégories de données Wi-Fi publiques n'est pas un produit externe. Le processus d'examen officiel ne s'est donc pas appliqué.

11) Cependant, notre enquête a dévoilé que la procédure d'élaboration de code de Google comprend un modèle et un processus selon lesquels le conseiller juridique en matière de produits doit examiner le code avant que celui-ci ne soit utilisé ou intégré à un autre produit de Google. Le modèle — un document qui explique la méthodologie — est pour ainsi dire obligatoire et constitue la première étape de la procédure d'élaboration d'un code.

12) L'enquête a aussi révélé que, dans le document établissant la procédure d'élaboration du code qui allait servir à capter les signaux Wi-Fi, l'ingénieur a cerné une ou plusieurs préoccupations relatives à la collecte. Ces préoccupations étaient liées au fait que Google pourrait obtenir suffisamment de données pour trianguler avec précision l'emplacement d'un utilisateur à un certain moment.

13) L'ingénieur a affirmé que ses préoccupations avaient des répercussions superficielles sur la vie privée. Il n'a pas envoyé ses documents sur l'élaboration du code au conseiller juridique en matière de produits aux fins d'examen - ce qui contrevient à la procédure de l'entreprise. Les facteurs relatifs à la vie privée du code n'ont donc jamais été évalués.

14) Nous avons aussi appris que les membres du service juridique en matière de produits de Google étaient des avocats qui avaient des antécédents professionnels dans divers secteurs du droit. Google soutient que ces juristes ont généralement une certaine expérience des questions liées à la protection des renseignements personnels dans le secteur privé.

15) Selon Google, les membres du service juridique en matière de produits assistent à la même séance de formation de base que tous les nouveaux employés de l'entreprise. En outre, ils participent à des réunions hebdomadaires sur des enjeux liés à la protection de la vie privée et à la sécurité. Google affirme également que la formation juridique continue obligatoire pour les conseillers juridiques de Google comprend la protection de la vie privée

B. Les circonstances entourant la collecte de données utiles et les essais techniques

16) Google permet à ses ingénieurs de consacrer 20 % de leur temps à des projets qui les intéressent. En 2006, un des ingénieurs a consacré ce temps à la création d'un code visant à prélever des échantillons de toutes les catégories de données Wi-Fi publiques.

5) Le 28 juin 2010, conformément au paragraphe 11(2) de la *Loi*, le Commissariat a demandé de visiter les locaux de Google à Mountain View (Californie). La visite sur place avait un double objectif : 1) examiner les données utiles recueillies par Google et 2) poser des questions précises aux représentants de l'entreprise, par exemple sur les circonstances de l'incident, l'isolement et le stockage des données utiles et les mesures d'atténuation et de prévention que Google prévoit mettre en œuvre.

6) Google a accepté une visite sur les lieux. Deux représentants spécialisés du Commissariat se sont ensuite rendus dans les locaux de Mountain View, le 19 juillet 2010. Bien que nos spécialistes aient passé en revue les données utiles, aucun représentant de Google n'était disponible pour répondre à nos questions à Mountain View. Google a plutôt répondu à nos questions générales en remplissant un questionnaire que nous lui avons transmis le 12 juillet 2010.

7) Le 18 août 2010, une téléconférence a eu lieu entre un avocat de Google et le Commissariat pour répondre à des questions supplémentaires.

8) Les résultats de notre enquête sur les trois plaintes déposées contre Google sont résumés dans les sections suivantes:

A. La participation du conseiller juridique en matière de produits de Google à l'examen des produits;

B. Les circonstances entourant la collecte de données utiles et les essais techniques;

C. La collecte de renseignements personnels;

D. L'isolement et le stockage des données utiles;

E. Les plans d'avenir de Google concernant ses services géodépendants;

F. Les répercussions des plans d'avenir sur la vie privée et les mesures d'atténuation et de prévention que Google prévoit prendre pour éviter une récidive.

A. La participation du conseiller juridique en matière de produits de Google à l'examen des produits

9) Google a expliqué qu'elle dispose d'un processus d'examen officiel pour chaque lancement de produit externe (c'est-à-dire un produit offert aux consommateurs). Ce processus prévoit qu'un conseiller juridique en matière de produits doit évaluer notamment les répercussions du produit sur la vie privée.

LETTRE DE CONCLUSIONS PRÉLIMINAIRE

Plaintes déposées en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques (la Loi)

1) Après avoir appris que les voitures de Google Street View avaient recueilli des données utiles transmises par des réseaux Wi-Fi non cryptés dans le cadre de la collecte de signaux Wi-Fi publics (des renseignements sur les identificateurs d'ensemble de services et des adresses MAC), le Commissariat à la protection de la vie privée du Canada a déposé trois plaintes contre Google inc. (Google) le 31 mai 2010, conformément au paragraphe 11(2) de la Loi.

2) Les trois plaintes sont les suivantes:

   i. Google aurait recueilli, utilisé ou communiqué des données utiles sans avis et consentement préalable ;

   ii. Google aurait recueilli des données utiles sans déterminer les fins de la collecte de renseignements personnels au préalable ;

   iii. Google aurait recueilli des données utiles au-delà de ce qui est nécessaire aux fins déterminées.

Résumé de l'enquête

3) Après que l'autorité allemande de protection des données à Hambourg a demandé de soumettre à une vérification les données Wi-Fi recueillies par les voitures de Google Street View au cours d'un projet fondé sur la localisation, Google a découvert en mai 2010 qu'elle avait recueilli des données utiles transmises sur des réseaux sans fil non protégés dans le cadre de ses activités de collecte de données Wi-Fi. Selon l'entreprise elle-même, cette collecte accidentelle semble avoir été causée par l'intégration d'un code élaboré en 2006 au logiciel utilisé pour capter les signaux Wi-Fi. Devant cette situation, Google a immobilisé ses voitures Street View, arrêté de recueillir des données sur les réseaux Wi-Fi le 7 mai 2010, et isolé et stocké toutes les données déjà recueillies.

4) Le 1er juin 2010, le Commissariat a écrit à Google pour aviser l'entreprise qu'il lançait une enquête concernant cette collecte de données utiles. Google a répondu le 29 juin 2010.

données. Si elles conservent des images non brouillées, elles doivent cependant limiter la période durant laquelle elles les gardent et les protéger avec des mesures de sécurité appropriées.

LE FACTEUR DÉCISIF

La technologie de l'imagerie à l'échelle de la rue peut comporter des avantages, mais ceux-ci ne doivent pas l'emporter sur votre vie privée.

C'est la raison pour laquelle nous encourageons les entreprises de technologie à prendre les moyens nécessaires pour que vous puissiez continuer à profiter de vos droits en matière de protection de la vie privée, même lorsque vous êtes simplement au parc, que vous promenez votre chien ou que vous profitez du soleil dans votre cour.

Fédéral

Commissariat à la protection de la vie privée du Canada

Provincial

Information and Privacy Commissioner of Alberta

Information and Privacy Commissioner for British Columbia

Commission d'accès à l'information du Québec

Le consentement peut être explicite ou implicite.

En général, selon les lois visant la protection de la vie privée dans le secteur privé, l'information et le consentement ne sont pas nécessaires aux fins journalistiques, artistiques ou littéraires. D'autres exceptions figurent dans les quatre lois sur la protection de la vie privée pertinentes, soit la *Loi sur la protection des renseignements personnels et les documents électroniques*, la *Personal Information Protection Act* (Colombie-Britannique), la (Alberta) et la .

Toutefois, dans le cas de certaines des nouvelles applications de l'imagerie à l'échelle de la rue, vous ne savez pas toujours quand votre photo est prise. C'est la raison pour laquelle nous croyons que les entreprises qui s'adonnent à ce type d'activité doivent déployer davantage d'efforts pour faire savoir aux citoyens qu'elles vont photographier les rues de leur ville, le moment où cela se produira, la raison de cette activité et le moyen par lequel ils peuvent demander à ce que leur photo ne soit pas versée dans la banque de données. Par exemple, les véhicules utilisés pour enregistrer l'information pourraient porter des marques visibles, et l'on pourrait utiliser une vaste gamme de moyens (communiqué de presse, médias régionaux, site Web du service) pour diffuser les renseignements sur les dates et emplacements de tournage, la raison pour laquelle on procède à ce dernier et la manière dont on peut communiquer avec l'entreprise pour obtenir davantage de renseignements. La plupart des gens ne s'attendent probablement pas à ce que leur photo soit prise par une entreprise dans le cours de leurs activités quotidiennes, mais cela peut les déranger moins s'ils ont le choix de planifier leur journée en conséquence.

LA DIMENSION DE LA PROTECTION DE LA VIE PRIVÉE ET VOTRE IMAGE EN LIGNE

Les applications de l'imagerie à l'échelle de la rue utilisent divers moyens pour photographier le paysage urbain. De façon générale, une caméra est montée sur un véhicule qui parcourt les rues de villes choisies. Les images peuvent ensuite être visualisées sur Internet.

Les commissaires à la protection de la vie privée ont tenu des discussions avec diverses entreprises pour renforcer les mécanismes de protection des personnes dont la photo a été prise. Nous croyons que toutes les entreprises qui offrent de telles applications doivent prendre des mesures pour mieux protéger votre vie privée.

En plus de demander aux entreprises d'être plus proactives et originales dans leurs communications avec le public pour veiller à ce que les Canadiennes et les Canadiens soient informés du moment où leurs villes — et par conséquent eux-mêmes — pourraient être photographiées, nous croyons qu'elles devraient adopter une attitude plus sensible au respect de la vie privée lorsqu'elles choisissent les endroits à photographier. Les personnes qui pénètrent dans des lieux, comme des refuges ou des cliniques d'avortement, où la confidentialité est d'une importance capitale ou qui en sortent veulent vraisemblablement conserver l'anonymat pour des raisons liées à leur vie privée ou à leur sécurité.

Les entreprises devraient également utiliser des technologies de brouillage efficaces et éprouvées des visages et des numéros de plaques d'immatriculation de façon à ce que les personnes ne puissent être identifiées lorsque leurs photos sont affichées sur Internet. Dans ces cas, les entreprises devraient offrir des mécanismes rapides et réactifs qui permettent de bloquer ou de retirer les images.

Les entreprises qui offrent ces applications d'imagerie doivent également avoir une bonne raison pour conserver les images originales et non brouillées dans leurs bases de

VOUS ÊTES PHOTOGRAPHIÉS
LA TECHNOLOGIE DE L'IMAGERIE À L'ÉCHELLE DE LA RUE, INTERNET ET VOUS

De nombreuses entreprises ont commencé à recueillir des images de lieux publics canadiens qui peuvent ensuite être vues sur Internet ou par d'autres moyens. Des personnes peuvent être captées sur ces images, parfois de façon non intentionnelle. Une des applications les plus connues est Street View de Google qui permet à ses utilisateurs d'effectuer des « visites virtuelles » de villes comme Paris, Londres, New York et, un jour, de grands centres urbains du Canada. En outre, Canpages fournit des images fixes provenant de caméras de circulation routière locale. D'autres applications ont également été élaborées pour des domaines comme la géomatique, l'arpentage, la cartographie et l'urbanisme.

Au Canada, les lois sur la protection des renseignements personnels dans le secteur privé visent ces applications de l'imagerie à l'échelle de la rue quand elles recueillent des images de personnes identifiables. Bien que les commissaires à la protection de la vie privée du Canada, de la Colombie-Britannique, de l'Alberta et du Québec reconnaissent la popularité de ces applications, ils ont également exprimé des réserves au fait que cette technologie permet non seulement de saisir des images d'endroits, mais également des images des personnes qui s'y trouvent.

Les commissaires croient que les Canadiennes et les Canadiens doivent être conscients des enjeux de protection de la vie privée que ces applications peuvent soulever.

LES PERSONNES DANS LES LIEUX PUBLICS

On croit souvent à tort qu'une entreprise n'a pas besoin de votre autorisation pour vous prendre en photo dans un lieu public.

En fait, la législation canadienne sur la protection des renseignements personnels prévoit, notamment, que vous devez être au courant lorsqu'on vous photographie à des fins commerciales et connaître l'utilisation qui sera faite de votre image. On doit également obtenir votre consentement . Il y a des exceptions à cette règle, mais elles sont très limitées et précises[4].

LISTE DES RECOMMANDATIONS

RECOMMANDATIONS

1. Compte tenu des profondes transformations qui touchent les médias sociaux et Internet en général, le Comité recommande que le Commissariat à la protection de la vie privée continue de faire preuve de vigilance pour bien protéger la vie privée des Canadiens dans ce contexte et se tenir au courant des questions qui préoccupent les Canadiens à ce sujet.

2. Le Comité soutient les recommandations présentées par la commissaire à la protection de la vie privée dans sa *Lettre de conclusions préliminaire* au sujet de la collecte de données Wi-Fi par Google et demande à Google d'appliquer ces recommandations dès que possible et d'ici l'échéance du 1er février 2011 fixée par la commissaire à la protection de la vie privée. Le Comité recommande que la commissaire à la protection de la vie privée communique avec lui dès qu'il aura reçu confirmation que Google s'est conformée aux recommandations précitées.

3. Le Comité recommande aussi que la commissaire à la protection de la vie privée l'avise de toute préoccupation qui pourrait être soulevée au sujet de la mise en application de ses recommandations par Google.

4. Le Comité recommande que la commissaire à la protection de la vie privée précise aux fournisseurs de technologie, comme ceux dont il a entendu le témoignage, l'importance d'avoir des programmes en bonne et due forme de formation sur la protection de la vie privée à l'intention de leurs employés.

5. Le Comité recommande que le Commissariat à la protection de la vie privée poursuive ses activités de sensibilisation – comme la publication de la fiche d'information *Vous êtes photographiés* — La technologie de l'imagerie à l'échelle de la rue, Internet et vous – pour informer le grand public sur ses droits en matière de protection de la vie privée et sur les risques que présentent les nouvelles technologies et les médias sociaux.

6. Enfin, le Comité reprend la recommandation formulée par la commissaire à la protection de la vie privée elle-même, à savoir que les innovateurs comme Google doivent intégrer les principes de la protection de la vie privée à la conception des nouveaux produits et consulter la commissaire, ainsi que, au besoin, ses homologues étrangers, de façon à garantir la protection de la vie privée dans le monde numérique.

nouveaux projets. Il leur faut cerner les risques éventuels pour la vie privée et les supprimer ou les réduire dès le début des nouveaux projets, au lieu de les affronter après coup à grands frais. Pour ce qui est de l'incident qui a impliqué Google, le Comité fait preuve d'un optimisme prudent, ayant bon espoir que l'entreprise progresse dans la bonne direction par sa décision de nommer Alma Whitten directrice de la protection de la vie privée, de donner de la formation sur la vie privée à ses employés et d'instaurer plus de mesures de contrôle de la vie privée en milieu de travail, comme la vérification de projets en cours d'élaboration. Le Comité compte bien que Google mettra en œuvre les recommandations de la commissaire à la protection de la vie privée sur la collecte de données Wi-Fi formulées dans la *Lettre de conclusions préliminaire* de celle-ci, et ce, d'ici l'échéance du 1er février 2011 fixée par la commissaire.

Le Comité note par ailleurs que son étude a permis de sensibiliser le Groupe Pages jaunes à l'importance de la protection de la vie privée et que celui-ci envisage maintenant de former ses employés à ce sujet et de consulter le Commissariat à la protection de la vie privée lors de la conception de ses produits.

Le Comité félicite la commissaire à la protection de la vie privée pour son apport dans ce dossier et pour son travail avec ses homologues étrangers en vue de l'intégration des principes de la « protection intégrée de la vie privée »[94] à la conception des nouveaux produits de l'ère numérique.

---

94 La « protection intégrée de la vie privée » est un concept élaboré par Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario, pour désigner l'intégration, par défaut, des considérations en matière de protection de la vie privée dans la technologie même : http://www.privacybydesign.ca/about/. À la 32e Conférence internationale des commissaires à la protection des données et de la vie privée tenue à Jérusalem, en Israël, du 27 au 29 octobre 2010, les commissaires ont approuvé la résolution sur la protection intégrée de la vie privée présentée par Mme Cavoukian et coparrainée par la commissaire à la protection de la vie privée du Canada, ainsi que par des commissaires d'autres pays : http://www.ipc.on.ca/french/resources/news-releases/news-releases-summary/default.aspx?id=992.

> Je confirme donc qu'à strictement parler, la caméra n'identifie pas vraiment un commerce. Celui-ci est simplement géocodé, ce qui permet au téléphone pointé dans la bonne direction de présenter un affichage correspondant[91].

M. Ramsay a précisé que, à sa connaissance, les services pour téléphones intelligents comme Canada Eye sont conformes aux lois et politiques canadiennes en matière de protection de la vie privée. Il a signalé que « nous donnons aux gens des itinéraires à suivre en nous fondant, encore une fois, sur des services offerts par des sociétés telles que Google et Microsoft[92] ». Autrement dit, la technologie de géolocalisation n'a pas été mise au point à l'interne par le Groupe Pages jaunes.

CONCLUSION

Après avoir entendu les témoignages de représentants de Google Canada, de Canpages et du Commissariat à la protection de la vie privée, le Comité est convaincu que toutes les parties concernées traitent avec sérieux les préoccupations de la population canadienne concernant la technologie de l'imagerie à l'échelle de la rue et la protection de la vie privée. Google et Canpages ont, de concert avec le commissariat à la protection de la vie privée, établi des pratiques exemplaires qui visent la communication d'avis aux résidants sur la période au cours de laquelle les véhicules passeront dans les rues, le brouillage obligatoire des visages et des signes distinctifs (comme les numéros des plaques d'immatriculation), la durée de conservation des images et les procédures d'élimination des images en cas de plainte. Le Commissariat a notamment assuré au Comité qu'il continuera de suivre l'évolution de la situation concernant la protection de la vie privée et l'imagerie à l'échelle de la rue pour assurer la conformité aux exigences des lois canadiennes en vigueur. Pour sa part, le Comité continuera de suivre l'évolution de la situation dans ce domaine, en y revenant au besoin.

Cependant, la collecte de données utiles Wi-Fi non protégées soulève une question plus générale : Dans quelle mesure le respect de la vie privée est-il pris en compte à l'étape de l'élaboration de nouvelles technologies? Comme l'a mentionné la commissaire, « la question, c'est pourquoi [Google] n'applique-t-elle pas les principes de protection des renseignements personnels dès le départ? Et pourquoi les contribuables canadiens ou les contribuables espagnols, etc., doivent-ils dépenser beaucoup de temps et d'efforts alors que ces entreprises devraient faire les choses correctement dès le début, avant de lancer leurs produits sur le marché[93]? »

Le Comité estime que les concepteurs de technologies doivent accorder une attention très particulière à la protection de la vie privée à l'étape de l'élaboration de leurs

---

91 *Ibid.*, 1705.

92 *Ibid.*

93 Jennifer Stoddart, commissaire à la protection de la vie privée du Canada, *Témoignages*, réunion n° 25, 19 octobre 2010, 1615, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4702609&Mode=1&Parl=40&Ses=3&Language=F.

> réseaux ou des données utiles Wi-Fi. Par conséquent, nous n'avons jamais été en possession de telles données.
>
> Les sociétés Yellow Media Inc., GPJ, Trader et Canpages sont déterminées à se conformer à la législation de protection de la vie privée qui s'applique dans notre secteur[87].

M. Ramsay et M. Aubut ont dit qu'ils pourraient fournir au Comité confirmation des technologies employées par leurs fournisseurs pour les produits Canpages[88].

En ce qui concerne la formation des employés du Groupe Pages jaunes sur la protection de la vie privée, M. Ramsay a dit qu'il n'en existait pas encore, mais que sa comparution et le témoignage de M^me^ Whitten de Google l'avaient convaincu de s'occuper de ce dossier[89].

M. Ramsay a indiqué que le Groupe Pages jaunes n'avait jamais directement consulté le Commissariat à la protection de la vie privée au sujet des problèmes potentiels que pourraient présenter ses produits, mais qu'il souhaitait que cela change. Il a dit : « Je peux vous dire cependant que je suis déterminé, avec un certain nombre de mes collègues, à explorer ce domaine et à adopter une approche proactive. Nous comprenons qu'en présence d'un monde de plus en plus numérique, beaucoup de ces questions vont passer au premier plan. Il est donc important pour nous d'être bien préparés et de nous montrer sensibles aux préoccupations légitimes des institutions canadiennes au chapitre de la protection de la vie privée[90]. »

En ce qui concerne Canada Eye, un service reposant sur la géolocalisation lancé par Canpages en mars 2010, M. Ramsay a expliqué ce qui suit :

> Je ne sais pas s'il y a des membres du comité qui ont sur eux un iPhone, mais il y a un bouton à pousser sur l'application Canpages. Je connais mieux l'application du GPJ, qui est un concurrent de Canpages. Il s'agit essentiellement de pointer la caméra de l'iPhone dans une certaine direction, ce qui permet d'afficher des noms d'entreprises au moyen du GPS de l'iPhone ou d'un autre téléphone intelligent [...] Je suppose que l'image est en quelque sorte un trucage, dans le sens que ce n'est pas vraiment ce que l'œil voit. C'est simplement que l'iPhone détecte la direction dans laquelle il est pointé et détermine en conséquence les commerces qui se trouvent dans cette direction.

---

87 François Ramsay, *Témoignages*, réunion n° 34, 25 novembre 2010, 1530, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Mode=1&Parl=40&Ses=3&Language=F.

88 *Ibid.*, 1710.

89 *Ibid.*, 1630.

90 *Ibid.*, 1645.

2. Où les données utiles ont-elles été stockées :

Les données utiles recueillies n'importe où dans le monde avant mai 2010, moment où le problème a été découvert et où la collecte a cessé, ont été stockées aux États-Unis et y sont encore.

Les disques durs des véhicules Street View qui n'avaient pas été traités au moment de la découverte du problème ont été mis en sécurité sur une base régionale. Ceux de l'Amérique du Nord, de l'Amérique du Sud et de l'Asie sont aux États-Unis et ceux de l'Europe et de l'Afrique sont en Europe.

3. Quelles données utiles ont été détruites :

Les données utiles désignées comme provenant des pays suivants avaient été détruites de façon sécuritaire à la date de la présente lettre : Irlande, Autriche, Danemark, Hong Kong et Royaume-Uni.

4. La société Google a-t-elle été soumise à des accusations au criminel ou à des sanctions ou pénalités administratives pour cette affaire quelque part dans le monde?

Non[86].

C. Groupe Pages jaunes (Canpages)

Le 25 novembre 2010, le Comité a entendu aussi François D. Ramsay, premier vice-président, conseiller juridique principal, secrétaire et responsable du respect de la vie privée et Martin Aubut, premier directeur, Commerce social, pour se renseigner sur les améliorations apportées au produit Vue de la rue (Street Scene) de Canpages (Pages jaunes) et déterminer comment l'entreprise intègre la protection de la vie privée à l'élaboration de ses produits.

Dans sa déclaration préliminaire, M. Ramsay a brièvement décrit le Groupe Pages jaunes, qui a fait l'acquisition de Canpages en juin 2010. Il a précisé que le produit Vue de la rue obtient ses données cartographiques aux termes de contrats de licence conclus avec deux sociétés, MapJack et Google. Après que Google a découvert qu'elle avait recueilli des données utiles Wi-Fi, le Groupe Pages jaunes a obtenu confirmation de la part de MapJack que cette dernière n'avait jamais recueilli de données de réseau ou de données utiles Wi-Fi :

Selon l'endroit où on se trouve dans notre univers de sites Web [Yellow Média Inc., le réseau de sociétés qui comprend le Groupe Pages jaunes, la société Trader et Canpages], on utilisera la technologie Street View de Google et de Microsoft, à part celle de MapJack, fournisseur traditionnel de Canpages.

Je suis heureux de confirmer au comité que MapJack, fournisseur du service Street Scene/Scènes de rue de Canpages, n'a pas été utilisé pour recueillir des données

---

86 Lettre de Jacob Glick envoyée par courriel au greffier du Comité, 9 décembre 2010.

> Nous en sommes aussi très conscients sur le plan interculturel. Nous voulons donc que notre examen de vie privée nous donne des perspectives venant de tous les coins de la planète où nos produits sont vus et utilisés. C'est en partie la raison pour laquelle je suis maintenant basée en Europe: je peux ainsi veiller personnellement à apporter un petit peu plus d'équilibre grâce à l'expérience que j'ai acquise aux États-Unis.
>
> Le Canada est certainement l'un des pays auxquels nous prêtons une très grande attention par suite des travaux de votre commissaire à la protection de la vie privée et de son influence sur la scène internationale. Nous comptons beaucoup sur les relations et les contacts étroits de Jacob avec le Commissariat. Nous faisons la même chose dans tous les pays où nous sommes présents[82].

Dans son témoignage du 25 novembre 2010, M. Glick a confirmé que Google n'avait pas encore détruit les données Wi-Fi qu'elle avait recueillies et qu'elle attendait pour cela les résultats d'une analyse des questions qui pourraient éventuellement empêcher la suppression immédiate des données :

> Nous faisons précisément ce que la commissaire a demandé. Nous avons entrepris une analyse de la législation tant canadienne qu'américaine liée au droit de la preuve et à d'autres questions pour déterminer la mesure dans laquelle les données peuvent être supprimées. Entre-temps, nous faisons exactement ce qu'elle a demandé en protégeant les données et en mettant en place les mesures de sécurité nécessaires[83].

M. Glick a ajouté que, « [e]n fin de compte, notre objectif est de détruire toutes les données. Nous n'en voulions pas au départ et nous n'en voulons pas aujourd'hui. Toutefois, nous voulons éviter de les détruire prématurément en suscitant encore plus de problèmes[84]. » M. Glick s'est engagé à fournir au Comité une liste des pays où Google fait l'objet de poursuites pénales ou de sanctions administratives en raison de la collecte de données utiles Wi-Fi[85].

Dans une lettre au Comité datée du 9 décembre 2010, M. Glick a fourni les réponses suivantes aux questions du Comité :

> **1. Dans quels pays la société Google a-t-elle recueilli par erreur des données utiles provenant de réseaux Wi-Fi non protégés :**
>
> États-Unis d'Amérique, Canada, une grande partie de l'Europe (Autriche, Belgique, République tchèque, Danemark, Finlande, France, Allemagne, Royaume-Uni, Grèce, Hongrie, Irlande, Italie, Luxembourg, Pays-Bas, Norvège, Pologne. Portugal, Roumanie, Espagne, Suède et Suisse), Australie, Hong Kong, Japon, Corée du Sud, Macao, Nouvelle-Zélande, Singapour, Taïwan, Brésil, Mexique et Afrique du Sud.

---

82 *Ibid.*, 1645.

83 Jacob Glick, *Témoignages,* réunion n° 34, 25 novembre 2010, 1605, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Mode=1&Parl=40&Ses=3&Language=F#Int-358090!.

84 *Ibid.*, 1620.

85 *Ibid.*, 1715.

comprendra une formation générale sur la sécurité et la protection des renseignements personnels, une formation sur un code de conduite et une formation plus ciblée et plus approfondie portant spécifiquement sur divers types d'activités :

> Le point le plus important sur lequel nous insisterons constamment dans le cadre de la formation, c'est que les ingénieurs ne doivent jamais faire eux-mêmes ce genre de jugement de valeur. Nous voulons les sensibiliser à l'environnement de la vie privée et aux préoccupations qu'elle soulève.
>
> Nous sommes également déterminés à leur faire comprendre les principes Google de protection de la vie privée, qui sont fondés sur la transparence, le contrôle et l'administration responsable. Nous voulons surtout leur apprendre à ne jamais perdre de vue les processus améliorés que nous mettons en place pour nous assurer d'avoir des mesures à sécurité intégrée et des procédures d'examen réfléchies et pour veiller à ce que les ingénieurs n'essaient pas de se substituer aux avocats pour régler certaines questions.
>
> [...]
>
> Nous avons l'intention de faire suivre aux ingénieurs nouvellement engagés une session assez importante de formation en protection de la vie privée dans les deux premières semaines qu'ils passent chez Google, avant qu'ils ne soient chargés d'écrire des programmes ou de développer des produits. Grâce à cette formation initiale, nous espérons jeter les fondations nécessaires pour qu'ils apprennent à qui ils doivent s'adresser et où se trouvent les ressources internes pouvant les aider à comprendre la vie privée et les processus que nous avons mis en place dans ce domaine. Nous espérons leur donner ainsi les éléments de base pour qu'ils trouvent rapidement et facilement des personnes à qui parler en cas de besoin.
>
> Pour ce qui est des autres ingénieurs qui ne seront pas passés par cette formation initiale donnée juste après l'embauche, nous organiserons une formation de suivi. Par-dessus tout, le processus que nous sommes en train d'améliorer et d'optimiser en ce moment permettra d'intégrer les deux volets de la formation pour qu'ils se renforcent mutuellement et fonctionnent bien ensemble.
>
> Le processus obligera les ingénieurs à passer par la formation à différentes étapes du cycle de vie de leurs projets. Comme on s'attend à ce qu'ils participent au processus, la formation leur permettra de savoir comment faire et les aidera à agir. L'objectif consiste très certainement à faire en sorte que les deux volets se renforcent l'un l'autre pour rendre le processus aussi efficace que possible[81].

M[me] Whitten a aussi expliqué comment Google se tient au fait des règles sur la protection de la vie privée en vigueur dans les divers pays où l'entreprise est active :

> Nous avons des experts locaux sur le terrain dans autant de pays que possible... en fait, dans la plupart des pays. En réponse à une question posée plus tôt, j'ai parlé de la nécessité de recourir à toutes sortes d'experts juridiques, techniques, etc.

---

81 *Ibid.*, 1625.

Préalablement à la comparution de M^me^ Whitten, Google a envoyé au Comité la notice biographique suivante à son sujet[77] :

> Alma Whitten a rejoint Google en 2003 et occupe actuellement le poste de directrice de la protection de la vie privée pour l'équipe d'ingénierie comme pour l'équipe de produit. À ce titre, elle est chargée de voir à ce que Google intègre à ses produits et ses pratiques internes des mesures de contrôle efficaces pour protéger la vie privée. Spécialiste de renommée internationale dans le domaine de la protection de la vie privée et de la sécurité, M^me^ Whitten a témoigné devant le Congrès des États-Unis et a comparu devant le Groupe de travail « article 29 » de la Commission européenne.
>
> M^me^ Whitten a été auparavant responsable de la sécurité appliquée puis responsable des outils de protection de la vie privée, affectation durant laquelle elle a mis sur pied les équipes qui ont mis au point des outils comme le Dashboard de Google.
>
> Avant d'entrer chez Google, M^me^ Whitten a publié un document technique connu sur le problème du manque de convivialité des mesures de sécurité informatique intitulé « Why Johnny Can't Encrypt », un des documents fondateurs de la recherche sur la convivialité mesures de sécurité. Elle continue de faire de la recherche, de rédiger des textes et de donner des conférences sur les méthodes de sécurité et de protection de la vie privée axées sur le facteur humain dans le cadre de son travail chez Google. M^me^ Whitten possède un doctorat en informatique de l'Université Carnegie Mellon.

Dans son témoignage, M^me^ Whitten a dit au Comité qu'elle avait « consacré ma carrière, comme universitaire et maintenant comme directrice de la protection de la vie privée chez Google, à un seul grand objectif: permettre aux utilisateurs d'Internet d'assumer le contrôle de leur vie privée et de leur sécurité par des moyens intuitifs, simples et utiles »[78] et a évoqué le projet de Google de renforcer ses mesures internes en matière de sécurité et de protection des renseignements personnels :

> Dans le cadre de mes responsabilités étendues, j'aurai la possibilité de superviser les équipes d'ingénierie et de produits et de collaborer avec elles pour veiller à ce que les considérations de sécurité et de protection de la vie privée soient intégrées dans la totalité de nos produits. Même si les fonctions qui correspondent à ce rôle sont lourdes, je suis sûre que je pourrai compter sur les ressources et le soutien interne nécessaires pour aider Google à faire mieux [...] Nous voulons être sûrs que chacun des nouveaux produits que nous mettons en service répond aux normes élevées de sécurité et de protection des renseignements personnels que nos utilisateurs attendent de nous[79].

M^me^ Whitten a expliqué que Google a l'intention d'offrir à ses employés une formation sur la protection de la vie privée adaptée aux responsabilités de chacun[80] qui

---

77 Lettre envoyée par courriel au greffier du Comité, 22 novembre 2010. On trouvera de plus amples informations sur Alma Whitten sur le site Web http://www.google.com/research/pubs/author32149.html. [traduction]

78 Alma Whitten, *Témoignages,* réunion n° 34, 25 novembre 2010, 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4822275&Mode=1&Parl=40&Ses=3&Language=F.

79 *Ibid.*, 1540.

80 *Ibid.*, 1600.

renseignements en prévoyant des vérifications internes indépendantes pour protéger la vie privée des utilisateurs[71].

Google est d'avis que les modifications apportées vont grandement améliorer ses mécanismes et contrôles et éviter ainsi que des incidents comme celui des données Wi-Fi se produisent à nouveau.

M. Glick s'est vu demander plusieurs fois en quoi consiste le poste de directeur de la protection de la vie privée chez Google et en quoi Alma Whitten est qualifiée pour ce poste[72]. Il n'a pas été en mesure de fournir une notice biographique de M^me^ Whitten au cours de la réunion, mais il a signalé qu'elle travaille dans l'entreprise depuis des années, qu'elle a un doctorat en informatique et en sécurité et qu'elle a publié de nombreux articles sur les questions d'informatique, de sécurité et de respect de la vie privée. C'est une sommité mondiale dans le domaine du respect de la vie privée et de la sécurité depuis plusieurs années. Elle travaille à Londres, au bureau britannique de Google[73].

D'après le témoignage de M. Glick, il semblerait que Google n'a pas encore supprimé les données utiles recueillies au Canada, car il n'a pas été dit clairement si elles devaient être conservées pour une raison ou une autre[74]. M. Glick a entrepris de vérifier si — et quand — les données utiles canadiennes seront supprimées[75] et si les lois américaines pourraient faire obstacle à leur élimination[76].

2. Audition de Jacob Glick et Alma Whitten le 25 novembre 2010 (par téléconférence)

Après avoir entendu M. Glick le 4 novembre 2010, le Comité a décidé d'entendre la nouvelle directrice de la protection de la vie privée chez Google, Alma Whitten, et d'interroger de nouveau M. Glick, le 25 novembre 2010, pour obtenir un complément d'information sur les mesures prises par Google à la suite de la collecte accidentelle de données Wi-Fi et en réponse à la *Lettre de conclusions préliminaire* de la commissaire à la protection de la vie privée parue le 19 octobre 2010. Les deux témoins ont comparu par voie de téléconférence, M^me^ Whitten depuis Londres et M. Glick, depuis Toronto.

---

71 *Ibid.*

72 Voir, par exemple, 1550 et 1555.

73 *Ibid.*, 1550.

74 *Ibid.*, 1600.

75 *Ibid.*

76 *Ibid.*, 1635.

l'idée d'utiliser les véhicules pour repérer les points d'accès Wi-Fi en vue des services géodépendants.

> C'est une pratique courante dans l'industrie que d'utiliser les points d'accès publics Wi-Fi comme points de repère pour renseigner les utilisateurs sur l'endroit où ils se trouvent. L'ingénieur a conçu le code du logiciel pour recueillir les données réseau Wi-Fi et, hélas, les données utiles également. Par données utiles, on veut désigner le contenu des transmissions. Google ne voulait pas de ces données utiles et croit qu'il ne sert à rien de les recueillir et qu'il est inacceptable de le faire. L'ingénieur aurait dû signaler aux avocats à l'interne, chez Google, ce plan de collecte des données utiles. Il ne l'a pas fait. S'il l'avait fait, Google aurait eu la possibilité de repérer et de régler le problème dès le début du programme. Le code a donc été déployé sur les véhicules de Street View. Le logiciel a fait ce qu'il était programmé pour faire et il a recueilli les données réseau et les données utiles Wi-Fi transmises sur des réseaux non cryptés[68].

En avril 2010, les autorités allemandes ont demandé à Google de vérifier les données Wi-Fi recueillies par ses véhicules Street View. La vérification a révélé que Google avait recueilli des données utiles Wi-Fi en plus des données de réseau. Selon M. Glick, « [a]vant d'annoncer publiquement ce que nous avions découvert, j'ai appelé moi-même la commissaire Stoddart pour l'informer du problème. Ensuite, Google a fait une annonce publique et présenté des excuses pour l'incident[69]. » L'entreprise a immobilisé ses véhicules Street View et isolé les données. M. Glick a indiqué que « personne n'a examiné les données utiles provenant du Canada sinon les enquêteurs de la commissaire à la protection de la vie privée et ceux qui ont facilité leur travail. Elles n'ont été communiquées à aucune tierce partie[70]. » Le témoignage de M. Glick ne permet pas de déterminer clairement si la collecte de données Wi-Fi n'a commencé qu'en avril ou si elle avait commencé avant.

M. Glick a confirmé que, le 22 octobre 2010, Google a apporté des modifications importantes à ses politiques et mesures de contrôle concernant le respect de la vie privée. Il a dit avoir parlé à la commissaire, M^me^ Stoddart, avant que les mesures suivantes soient annoncées publiquement :

> D'abord, Google a nommé M^me^ Alma Whitten au poste de directrice de la protection de la vie privée pour veiller à ce que nous intégrions à nos produits et à nos pratiques internes des contrôles efficaces pour protéger la vie privée. M^me^ Whitten est une spécialiste internationalement reconnue dans les domaines de la protection de la vie privée et de la sécurité en sciences informatiques. Deuxièmement, nous améliorons notre formation de base en matière de protection de la vie privée en mettant un accent particulier sur la collecte, la manipulation et l'utilisation responsables des données. Enfin, Google ajoute de nouvelles garanties à son système actuel d'application de la protection des

---

68 *Ibid.*

69 *Ibid.*

70 *Ibid.*

B. Google Canada

1. Audition de Jacob Glick le 4 novembre 2010

Lorsqu'il a témoigné devant le Comité le 4 novembre 2010, Jacob Glick, conseiller en matière de politique au Canada pour Google, a parlé de l'outil Street View de Google et aussi de la collecte de données utiles Wi-Fi[63].

Au sujet de Street View, M. Glick a mentionné que Google a « tenu compte de toutes les préoccupations que le comité et la commissaire à la protection de la vie privée ont cernées. Nous avons appliqué la technologie de brouillage la plus perfectionnée pour masquer les visages et les plaques minéralogiques sur toutes nos images. Tous peuvent demander à Google de retirer les images d'eux-mêmes, de leur maison, de leurs enfants ou de leur voiture dans Street View. Enfin, après un an, nous intégrons ce brouillage de façon permanente[64]. » Il a ajouté que les Canadiens sont de fervents utilisateurs de Street View. « En chiffres absolus, ils sont au troisième rang des plus grands utilisateurs de ce produit dans le monde, derrière les États-Unis et le Royaume-Uni. Depuis le lancement, les Canadiens de tout le territoire se servent de cette cartographie de nouvelle génération pour tracer le parcours à suivre pour aller au magasin, faire la promotion de leur entreprise locale, vendre leur maison et explorer leur pays en ligne[65]. »

En ce qui concerne la collecte de données utiles Wi-Fi, M. Glick a précisé qu'elle n'avait pas de lien avec le produit Street View, mais que les véhicules Street View servaient de moyens de collecte. Il a présenté ses excuses au nom de Google, mentionnant que « ce qui s'est passé n'est pas conciliable avec notre engagement de servir les usagers d'Internet[66] ». Il a signalé que Google n'a recueilli « aucune donnée utile transmise par réseau crypté. Google ne voulait utiliser les données d'aucune manière, et elles n'ont servi dans aucun de ses produits ou services. Aucune donnée utile canadienne n'a été cédée ni communiquée à des tiers. Les données ont été isolées et mises en sécurité[67]. »

Pour ce qui est de savoir comment des véhicules Street View de Google en sont venus à recueillir des données utiles Wi-Fi, M. Glick a dit qu'en 2007, à l'époque où Google se préparait à lancer Street View et déployait ses véhicules partout dans le monde pour appliquer la technologie de l'imagerie à l'échelle de la rue, un de ses ingénieurs a eu

---

63 Jacob Glick, *Témoignages*, réunion n° 30, 4 novembre 2010, 1530, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4764635&Mode=1&Parl=40&Ses=3&Language=E.

64 *Ibid.*

65 *Ibid.*

66 *Ibid.*

67 *Ibid.*

> Je pense que nous avons toutes les raisons de le croire. Même si Google ne nous a pas donné de réponses officielles, nous avons pris connaissance des réponses dans la presse, comme vous tous, réponses qui portaient sur les mesures concrètes que les gens de Google ont déjà prises. Dans le cadre de notre enquête, nous avons pris connaissance des mesures qui avaient déjà été prises pour entamer le processus de mise en place de structures de gouvernance adéquates au sein de l'organisation, qui est un géant mondial, comme vous le savez. La date du 1er février a été choisie avec soin, compte tenu du délai raisonnable non seulement pour apporter ces changements, mais également pour obtenir des preuves concrètes du fait qu'ils auront été apportés à l'échelle mondiale. C'est la raison pour laquelle cette date a été choisie. Nous avons très bon espoir d'obtenir une réponse positive plus tôt, et nous en serions très heureux. Nous sommes assez persuadés que tout cela va bien se terminer[60].

Mme Kosseim a aussi mentionné que, pour le moment, le Commissariat à la protection de la vie privée est satisfait des mesures de protection de la vie privée appliquées pour les technologies Street View de Google et Scène de rues de Canpages, abstraction faite de la collecte de données utiles Wi-Fi, qui est un cas distinct :

> En ce qui concerne la technologie d'imagerie à l'échelle de la rue de Google et de Canpages, je veux simplement préciser que, dans un cas comme dans l'autre, les applications n'ont jamais fait l'objet d'une enquête de la commissaire [...] Cependant, d'après la correspondance et la réponse des organisations, les deux ont fait beaucoup de choses pour se plier aux recommandations de la commissaire ou pour poursuivre leurs activités en harmonie avec celles-ci, et elles ont notamment avisé les habitants des quartiers avant de les visiter, discuté avec les intervenants et les groupes vulnérables, mis au point des procédures de retrait des images ainsi que des mécanismes de conservation et de suppression et d'autres mécanismes de protection du genre. Ainsi, d'après cette correspondance, il se fait beaucoup de choses. Évidemment, les avis pourraient toujours être améliorés, comme la technologie qui permet de rendre les images floues peut toujours être améliorée, mais, jusqu'à maintenant, il y a eu énormément d'améliorations et de mesures qui ont été prises qui vont dans le sens de ce que la commissaire souhaitait[61].

En conclusion, Mme Kosseim a adressé une grande recommandation aux entreprises, comme Google, Canpages et Facebook, qui ont recours à de nouvelles technologies pour compiler, traiter et communiquer des renseignements, à savoir que ces entreprises doivent adopter le principe de la prudence face aux répercussions possibles sur la vie privée. Le Commissariat espère que les organisations qui conçoivent, élaborent et déploient des technologies de l'information dont tous les Canadiens bénéficient prendront « des mesures proactives dès le départ pour cerner les risques, les évaluer et les gérer avant le déploiement à grande échelle de ces technologies[62] ».

---

60 *Ibid.*.

61 *Ibid.*, 1705.

62 *Ibid.*, 1705.

faisait[53] ». Google a expliqué que son objectif était d'améliorer ses « services géodépendants[54] ».

M[me] Kosseim a poursuivi en disant que la collecte de signaux Wi-Fi n'était pas liée au produit Street View en soi, mais que, pour des raisons de commodité, Google se servait de ses véhicules Street View pour recueillir les données Wi-Fi. Google a dit au Commissariat à la protection de la vie privée en avril 2010 qu'elle était en train d'installer des antennes sur le toit des véhicules Street View pour recueillir et capter en même temps les signaux radio Wi-Fi des environs[55].

C'est seulement en mai 2010, après avoir reçu des demandes d'information supplémentaires de la part de l'organisme allemand de protection des renseignements personnels, que Google s'est aperçue qu'elle recueillait sans le savoir des données utiles Wi-Fi[56]. Comme précisé dans la *Lettre de conclusions préliminaires*, Google a immobilisé ses véhicules Street View et arrêté de recueillir des données sur les réseaux Wi-Fi le 7 mai 2010 et a isolé et stocké toutes les données déjà recueillies.

D'après les résultats de son enquête, le commissariat n'avait pas de raison de croire que les données utiles Wi-Fi recueillies accidentellement par Google avaient été utilisées à des fins inappropriées[57].

Le commissariat a cependant reconnu que la simple collecte de renseignements sur l'accès Wi-Fi peut en soi poser d'éventuelles difficultés sur le plan de la vie privée. Comme l'a mentionné Andrew Patrick : « Si l'information au sujet de la présence d'un point d'accès à un réseau Wi-Fi peut être liée à une personne, en soi ou en rapprochant cette information d'autres éléments d'information, alors cela pourrait devenir de l'information personnelle et pourrait donc être source de préoccupation pour nous[58]. » Le commissariat ne dispose pas de renseignements précis sur les services géodépendants que Google est en train de mettre au point grâce à la collecte de signaux radio Wi-Fi[59].

M[me] Kosseim a dit dans l'ensemble qu'elle avait toutes les raisons de croire que Google appliquera les recommandations de la commissaire formulées dans la lettre de conclusions préliminaire :

---

53 *Ibid.*, 1555.

54 *Ibid.* Comme précisé plus haut, un « service géodépendant » est un service d'information et de divertissement accessible au moyen d'un appareil mobile dans le réseau mobile et qui tire parti de la capacité d'utiliser la position géographique de l'appareil.

55 *Ibid.*

56 *Ibid.*

57 *Ibid.*, 1605.

58 *Ibid.*

59 *Ibid.*, 1610.

> [...] Google avait recueilli des renseignements personnels de manière inappropriée à partir de réseaux sans fil non sécurisés. Dans certains cas, ces renseignements personnels étaient de nature très délicate, notamment des courriels au complet, des noms d'utilisateur et mots de passe, ainsi que des renseignements sur les troubles médicaux de personnes particulières. Malheureusement, cette collecte de données par inadvertance est le fruit d'une erreur qui aurait pu être facilement évitée si Google avait respecté ses propres procédures.
>
> Essentiellement, ce qui est arrivé, c'est que l'ingénieur qui a élaboré le code en vue d'échantillonner des catégories de données Wi-Fi diffusées publiquement a inclus également un code permettant la collecte de données utiles, croyant que ce type de renseignements pourrait servir un jour à Google. L'ingénieur a déterminé des préoccupations à son avis « superficielles » en matière de vie privée, mais, contrairement à la procédure de la société, il a omis de porter ses préoccupations à l'attention du conseil juridique en matière de produits, dont la responsabilité aurait été de les traiter et de les résoudre avant le lancement du produit[49].

Comme indiqué plus haut[50], la commissaire a recommandé que Google réexamine et améliore la formation offerte à tous ses employés au sujet du respect de la vie privée et instaure un modèle global de gouvernance qui garantit que les procédures nécessaires au respect de la vie privée ont été suivies avant le lancement d'un produit. Elle a de plus recommandé que Google supprime les données utiles recueillies au Canada dans la mesure où les lois canadiennes et américaines l'autorisent à le faire[51].

M[me] Kosseim a indiqué que la commissaire à la protection de la vie privée avait envoyé une « lettre de conclusions préliminaire » sur la collecte de données Wi-Fi. La commissaire veut des preuves que les recommandations ont été appliquées avant de mettre un terme à l'enquête et de « clore le dossier ». Autrement dit, elle veut une « mise en œuvre concrète, et pas de simples engagements[52] ».

M[me] Kosseim a ensuite précisé la façon dont le Commissariat à la protection de la vie privée avait été informé que Google recueillait des données utiles et des signaux Wi-Fi. Il avait reçu en avril 2010 un avis de Google l'informant que « l'entreprise avait l'intention de recueillir des signaux radio diffusés publiquement par des réseaux Wi-Fi et qu'elle le

---

49 Ibid.

50 Voir « Collecte, par Google, de données utiles dans des réseaux Wi-Fi non protégés et conclusions préliminaires du Commissariat à la protection de la vie privée ».

51 Patricia Kosseim, *Témoignages,* réunion n° 28, 28 octobre 2010, 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4739584&Language=F&Mode=1&Parl=40&Ses=3..

52 *Ibid.*, 1540.

moment où M^me^ Denham a comparu devant le Comité. Il a reçu des appels de la part de personnes souhaitant faire retirer leurs images de Street View, et celles-ci ont été renvoyées à Google et aucune, jusqu'à maintenant, n'est revenue au commissariat pour présenter une plainte officielle[44].

Quand on lui a demandé si le Commissariat à la protection de la vie privée estime que la politique de brouillage de Google répond aux normes des lois sur la protection des renseignements personnels par les entreprises au Canada, M^me^ Denham a affirmé que la technologie de brouillage de Google pourrait être meilleure : « Google nous a dit que sa technologie de brouillage est efficace à 98 p. 100. C'était avant la mise en marche du système. Nous avons constaté nous-mêmes que beaucoup de visages n'ont pas été brouillés. Google s'est engagé à améliorer le brouillage et c'est l'une des raisons pour lesquelles elle veut conserver les images pendant un an. Elle travaille sur l'amélioration de la technologie de brouillage. » La commissaire à la protection de la vie privée est satisfaite de ce délai d'un an[45].

CE QUE LE COMITÉ A ENTENDU : SUITE DES TÉMOIGNAGES — COLLECTE DE DONNÉES WI-FI PAR GOOGLE

A. Commissariat à la protection de la vie privée du Canada

Patricia Kosseim, avocate générale au Commissariat à la protection de la vie privée du Canada, a comparu devant le Comité le 28 octobre 2010 pour parler de l'enquête effectuée sur la collecte par inadvertance de données Wi-Fi par Google et qui a débouché sur l'envoi de la *Lettre de conclusions préliminaire* le 19 octobre 2010[46]. Elle a aussi fait le point sur les conséquences de la technologie d'imagerie à l'échelle de la rue pour la vie privée. Elle était accompagnée de Daniel Caron, conseiller juridique, Direction des services juridiques, des politiques et des affaires parlementaires, et d'Andrew Patrick, analyste de recherche en technologie de l'information.

Dans ses observations préliminaires, M^me^ Kosseim a résumé l'enquête du Commissariat sur la collecte accidentelle[47] de données utiles Wi-Fi non protégées par des véhicules Street View de Google. Elle a expliqué que les données utiles sont des renseignements sur les communications transmises dans les réseaux sans fil[48]. L'enquête a fait ressortir ce qui suit :

---

44 *Ibid.*, 0930, 1025.

45 *Ibid.*, 1025.

46 Commissariat à la protection de la vie privée du Canada, *Lettre de conclusions préliminaire*, 19 octobre 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_f.cfm.

47 Suivant les propres termes de Patricia Kosseim.

48 Patricia Kosseim, *Témoignages*, réunion n° 28, 28 octobre 2010, 1535, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4739584&Language=F&Mode=1&Parl=40&Ses=3.

continue de tenir à assurer que l'utilisation commerciale de cette technologie garantit « la protection de la vie privée des citoyens en veillant à ce que la technologie respecte les exigences de la LPRPDE en matière de connaissance, de consentement, de mesures de sauvegarde et de conservation limitée des renseignements[41] ».

De l'avis du commissariat, les sociétés devraient informer les citoyens de leur intention de photographier dans la rue en leur indiquant où et quand elles le feront, en plus de leur expliquer comment ils peuvent demander le retrait de leurs images s'ils ne veulent pas qu'elles soient diffusées en ligne. Les visages et les plaques d'immatriculation doivent être brouillés de façon à ce que les personnes puissent rester anonymes ou du moins ne pas être identifiables. Les sociétés doivent se doter de moyens efficaces et rapides de retirer les images des citoyens l'ayant demandé. Les images non brouillées conservées à des fins commerciales légitimes devraient être protégées au moyen de mesures de sécurité appropriées, et les données brutes ne devraient pas être conservées indéfiniment[42].

M[me] Denham a signalé que les fournisseurs de services qui ont comparu devant le Comité ont apporté des améliorations à ce chapitre. En août 2009, Google a convenu avec le Commissariat à la protection de la vie privée et d'autres commissaires à la protection des données en Europe qu'elle devait supprimer les images non brouillées au bout d'un an. Comme l'a dit M[me] Denham lors de son témoignage :

> L'une des plus vives controverses que nous avons eues dans nos discussions avec Google et Canpages concernait ce que devient l'image brute, non brouillée, conservée dans des bases de données aux États-Unis. Au début, Google était réticente à fixer une période de conservation limitée. Ensuite, au mois d'août, la société est convenue avec nous et avec d'autres commissaires de protection des renseignements personnels en Europe que les images non brouillées devraient être supprimées au bout d'un an. Elle nous a donné des justifications pour vouloir les conserver pendant un an et nous les avons acceptées. Google s'est également engagée à nous permettre de visiter ses installations afin de voir comment se fait la suppression ou l'anonymisation permanente des données au bout d'un an. C'était l'une de nos principales préoccupations au sujet de ce service[43].

M[me] Denham a également fait savoir au Comité que depuis le lancement de Street View de Google au début d'octobre 2009, le Commissariat à la protection de la vie privée a reçu seulement une dizaine de demandes d'information de la part de Canadiens et une seule plainte, laquelle a été réglée. La plainte provenait d'une personne qui estimait avoir été photographiée. Elle a été réglée lorsque Google a accepté de supprimer en permanence l'image de l'homme de la base de données, de sorte que le commissariat n'a jamais fait de recommandation publique. Le Commissariat à la protection de la vie privée n'avait pas reçu de plaintes concernant l'efficacité de la procédure de retrait de Google au

---

41 *Ibid.*

42 *Ibid.*, 0905.

43 *Ibid.*, 0930.

d'immatriculation, seront brouillés sur les images originales avant qu'elles ne soient mises en ligne. Le procédé de brouillage que nous employons est une technologie que nous-mêmes avons mise au point et elle est irréversible par les utilisateurs. Les images originales sont détruites après avoir été brouillées et avant d'être mises en ligne. Il n'est donc pas possible de récupérer les images originales après coup.

Les utilisateurs peuvent aussi communiquer à tout moment leurs inquiétudes au sujet des images en cliquant sur le lien « signaler une préoccupation » qui se trouve sur toute image de l'application Scène de rue. À la demande d'un utilisateur, Canpages offrira de brouiller l'image d'une personne, d'un véhicule, d'une fenêtre, d'un édifice, d'un animal — il suffit d'en faire la demande. Bien que les lois visant à protéger la vie privée ne soient pas nécessairement adaptées aux nouvelles technologies, qui évoluent rapidement, Canpages désire adopter une approche proactive afin de répondre positivement à toute préoccupation qui pourrait être soulevée au sujet de ce service.

[...]

Canpages a ouvert un dialogue avec le public, les divers commissariats à la protection de la vie privée et avec M. Pierre Poilievre, le député qui a déposé une motion devant ce Comité pour que ce dernier examine la question de la protection de la vie privée.

En conclusion, Canpages s'engage à collaborer immédiatement et en permanence avec les différents acteurs afin de régler tout problème potentiel lié à la protection de la vie privée qui pourrait résulter de ses innovations dans le domaine de la recherche locale[38].

Après ses observations préliminaires, M. Vincent a parlé, entre autres choses, de la technologie de brouillage employée par la société afin d'assurer l'anonymat des passants et des lieux sensibles. Il a précisé qu'avec les versions précédentes de la technologie de brouillage, il était plus facile de débrouiller l'image, mais la nouvelle version utilisée par la société est beaucoup plus puissante et le procédé de brouillage est irréversible. Il a aussi précisé que les versions d'origine de toute image qui doit être brouillée sont détruites et remplacées par la version floutée par application de la technologie[39].

C. Commissariat à la protection de la vie privée du Canada

Elizabeth Denham, commissaire adjointe au Commissariat à la protection de la vie privée du Canada, a comparu devant le Comité le 22 octobre 2009. M[me] Denham a informé le Comité que LPRPDE est une loi neutre sur le plan technologique qui est « un outil dynamique, moderne et efficace pour rehausser le droit à la vie privée des citoyens » qui a été conçu pour réagir à des situations comme « la collecte et [...] l'utilisation commerciales de renseignements personnels par la technologie de l'imagerie au niveau de la rue[40] ». Tout en sachant que de nombreux services utilisant l'imagerie au niveau de la rue sont très prisés de la population, le Commissariat à la protection de la vie privée

---

38 *Ibid.*

39 *Ibid.*, 1620, 1625 et 1720.

40 Elizabeth Denham, *Témoignages*, réunion n° 32, 22 octobre 2009, 0900, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=F.

excessive », après quoi ces images non brouillées seront floutées de façon permanente afin de les rendre complètement anonymes (au lieu de les éliminer[33]). En date de juin 2009, Google n'avait pas fixé de calendrier exact pour la conservation des images non brouillées[34]. M. Lister a signalé que Google informera le Comité du délai précis quand l'entreprise aura « une réponse exacte et raisonnable[35] ». Après la comparution de M. Lister devant le Comité, Google a convenu avec le Commissariat à la protection de la vie privée de conserver les images non brouillées pour une période d'un an[36].

B. Canpages

Lorsqu'il a comparu devant le Comité le 17 juin 2009, Olivier Vincent, président et chef de direction de Canpages, a expliqué la fonction de l'outil Scène de rues de Canpages qui vise principalement les zones commerciales : « Pleinement intégrée avec sa plate-forme de recherche Canpages.ca, l'application Scène de rues permet aux utilisateurs de consulter des photos panoramiques prises au niveau de la rue afin qu'ils puissent non seulement repérer les résultats de leur recherche sur une carte géographique, mais aussi voir les résultats de leur recherche à haute résolution dans un environnement local. Par exemple, les utilisateurs peuvent « marcher virtuellement » à travers les rues d'une ville et se rendre jusqu'à un restaurant local ou un hôtel particulier. Ils peuvent ainsi voir l'extérieur du restaurant recherché avant de faire la réservation, ou encore vérifier s'il est possible de stationner dans la rue ou dans un parc de stationnement disponible à proximité[37]. »

En ce qui concerne les préoccupations au sujet de la protection de la vie privée que soulève l'utilisation, par Scène de rues, d'images et de technologies de l'imagerie, M. Vincent a déclaré ce qui suit :

> Canpages est d'avis que le respect de la vie privée est une priorité essentielle. Ainsi nous sommes sensibles aux préoccupations de certains concernant la possibilité que la vie privée de personnes photographiées pendant la préparation des données requises pour le service Scène de rue pourrait être atteinte. Canpages est résolu à garantir à tous que leur vie privée sera respectée et a d'ailleurs annoncé publiquement son engagement en ce sens par la publication de sa politique de protection de la vie privée relative au service Scène de rue.
>
> Nous nous engageons donc à prévenir le public avant tout prochain tournage. Les visages des personnes et d'autres éléments reconnaissables, tels que les plaques

---

33 *Ibid.*, 1610.

34 *Ibid.*, 1650.

35 *Ibid.*, 1715.

36 Elizabeth Denham, *Témoignages,* réunion n° 32, 22 octobre 2009, 0930, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4159599&Mode=1&Parl=40&Ses=2&Language=F.

37 Olivier Vincent, *Témoignages,* réunion n° 29, 17 juin 2009, 1555, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=F&Mode=1&Parl=40&Ses=2.

> d'une image. Ainsi n'importe quel particulier peut demander à faire disparaître une image de lui-même, de membres de sa famille, de sa voiture ou de sa maison. Ce retrait est accordé même si ces éléments de l'image ont déjà été brouillés. Nous traitons des demandes de retrait tous les jours dans une multiplicité de langues différentes et le délai d'exécution de chaque demande est à la fois court et efficace.
>
> Un autre aspect important des efforts que nous déployons afin de garantir la protection de la vie privée est notre engagement à travailler avec les intervenants clés dans chaque pays afin de recenser et de contacter des organismes locaux pertinents avant le lancement du service. Ainsi notre équipe peut travailler en collaboration avec les intervenants clés canadiens pour leur fournir tous les détails importants au sujet de l'outil Street View, y compris la procédure à suivre pour faire brouiller ou enlever l'image de leur organisme.
>
> Nous sommes également en train de créer un système qui garantira que, le jour du lancement de Street View au Canada, nous aurons plus de personnel de disponible pour répondre aux demandes de retrait.
>
> Permettez-moi donc de conclure en disant que, comme c'est le cas pour beaucoup de technologies de pointe, notre défi, en ce qui concerne Street View, consiste à établir le bon équilibre entre les fonctions d'un outil sophistiqué que nous voulons très utile et l'utilisation appropriée des données que nous réunissons pour nous permettre d'offrir de tels services[29].

M. Lister a comparu devant le Comité avant le lancement de l'outil Street View au Canada en octobre 2009. À l'époque, il a informé le Comité que Google travaillait de près avec le Commissariat à la protection de la vie privée afin de s'acquitter de ses obligations juridiques et en matière de protection de la vie privée avant le lancement de Street View[30]. En réponse aux préoccupations concernant la possibilité que Street View viole la vie privée des particuliers à l'intérieur de leurs domiciles ou voie à l'intérieur de lieux sensibles comme des refuges pour femmes, M. Lister a signalé que les images Street View sont captées à l'extérieur de lieux publics : « [Street View] vise à améliorer la cartographie et à capter des images de bâtiments et de points de repère qui sont accessibles au public. Donc, il n'est pas nécessaire de voir l'intérieur; la définition même du produit n'inclut pas cet élément, et Google ne fait pas ce genre de chose[31]. »

S'agissant de politiques de conservation et d'élimination, les images de Google sont conservées dans des « fermes de serveur » sûres, dont la plupart semblent être situées aux États-Unis[32]. En ce qui concerne les images d'origine non brouillées, M. Lister signale que Google conserve les images claires en vue d'améliorer ses produits, c'est-à-dire pour améliorer les capacités de reconnaissance de la technologie de brouillage. Il a ajouté que Google a décidé de revoir sa politique de conservation des données afin de conserver les images non brouillées pendant « une période suffisante mais non

---

29 *Ibid.*

30 *Ibid.*, 1605, 1650.

31 *Ibid.*, 1630.

32 *Ibid.*, 1625.

charcuterie locale, boulangerie du coin, Starbucks ou Tim Hortons —, et d'obtenir ensuite les indications à suivre et la distance vers toutes les entreprises de cette catégorie dans le voisinage. En fait, Canada Eye est une application qui repère les entreprises des environs et qui renseigne sur la façon de s'y rendre en temps réel[26]. »

En juin 2010, le Groupe Pages jaunes a fait l'acquisition de Canpages pour environ 225 millions de dollars canadiens[27].

CE QUE LE COMITÉ A ENTENDU : PREMIERS TÉMOIGNAGES — LES APPLICATIONS D'IMAGERIE À L'ÉCHELLE DE LA RUE DE GOOGLE ET DE CANPAGES

A. Google Canada

Jonathan Lister, directeur général et chef de Google Canada, a comparu devant le Comité le 17 juin 2009. Dans ses observations préliminaires, M. Lister a souligné que Street View de Google « représente manifestement un produit qui change la façon dont les gens perçoivent les cartes [...] la grande innovation qu'offre l'outil Street View de Google est sa capacité de marier des images de la rue à des cartes numériques pour fournir un produit de qualité supérieure aux utilisateurs d'Internet[28] ».

En ce qui concerne les obligations juridiques et de protection de la vie privée qui incombent à Google dans divers pays, M. Lister a déclaré ce qui suit :

> D'abord, Google respecte les lois de tous les pays dans lesquels Street View est implanté. Les images que nous mettons à la disposition du public montrent simplement ce que n'importe qui pourrait voir en s'engageant dans une rue publique. Les images auxquelles on a accès grâce à Street View représentent un instantané et ont souvent été prises au cours de la dernière année. Il ne s'agit pas d'images en temps réel. Même si nous recueillons des images prises uniquement dans des lieux publics, nous savons depuis toujours que des passants peuvent être inclus dans nos images par inadvertance. Ainsi Google a investi d'importantes ressources dans la mise au point d'un procédé d'identification et de brouillage de certaines caractéristiques d'une image — par exemple, les visages et les plaques d'immatriculation — qui est le plus avancé du monde [...].
>
> Une autre composante clé des systèmes de protection de la vie privée que nous avons incorporés dans l'outil Street View est son système de demande de retrait d'images qui est facile à utiliser. Chaque image publiée dans Street View contient un lien « signaler un problème » qui renvoie les utilisateurs à une page où ils peuvent demander le retrait

---

26 « Canpages Brings "Augmented Reality" Local Search to the iPhone 3GS », 10 mars 2010, http://www.benzinga.com/pressreleases/m166514/canpages-brings-augmented-reality-local-search-to-the-iphone-3gs.

27 Yellow Media Inc., *Yellow Pages Group Finalizes Acquisition of Canpages*, 23 juin 2010, http://corporate.canpages.ca/media/Yellow%20Pages%20Group%20Finalizes%20Acquisition%20of%20Canpages.pdf.

28 Jonathan Lister, *Témoignages*, réunion n°29, 17 juin 2009, 1550, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004122&Language=F&Mode=1&Parl=40&Ses=2.

a. Responsabilité : une organisation est responsable des renseignements personnels qu'elle a en sa possession et doit charger une ou des personnes responsables de s'assurer de la conformité de ladite organisation aux principes suivants.

b. Détermination des fins de la collecte de renseignements : les fins de la collecte de renseignements doivent être précisées par l'organisation avant la collecte ou au moment où elle a lieu.

c. Consentement : la personne doit être informée et avoir donné son consentement pour que les renseignements personnels la concernant soient recueillis, utilisés ou communiqués, à moins qu'il ne soit pas approprié de le faire.

d. Limitation des collectes : la collecte de renseignements personnels se limitera à ce qui est nécessaire aux fins précisées par l'organisation. Les renseignements seront recueillis à l'aide de moyens loyaux et licites.

e. Limitation de l'utilisation, de la communication et de la conservation : les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'autorise. Vous ne devez conserver les renseignements personnels qu'aussi longtemps que nécessaire à la réalisation des finalités déterminées.

f. Exactitude : les renseignements personnels doivent être aussi exacts, complets, et mis à jour que nécessaire aux fins pour lesquelles ils pourraient être utilisés.

g. Mesures de sécurité : les renseignements personnels sont tenus d'être protégés par des mécanismes de sécurité adaptés à la sensibilité des informations.

h. Transparence : une organisation doit rendre facilement accessibles à toute personne des renseignements précis sur ses politiques et pratiques en matière de gestion des renseignements personnels.

i. Accès aux renseignements personnels : toute personne qui en fait la demande doit être informée du fait que vous possédez des renseignements personnels à son sujet, de l'usage que vous en faites ou entendez faire, ainsi que des tiers à qui ils sont communiqués, et doit se voir accorder le droit d'accéder à ces renseignements. Lorsqu'une personne démontre que des renseignements personnels la concernant sont inexacts et incomplets, vous devez apporter les corrections ou les modifications nécessaires.

j. Possibilité de porter plainte contre le non-respect des principes : toute personne doit pouvoir contester la conformité aux principes susmentionnés auprès de la ou des personnes responsables chargées de s'assurer de la conformité de l'organisation.

3. Canada Eye

En mars 2010, Canpages a lancé Canada Eye, application iPhone gratuite de « réalité augmentée ». Canada Eye permet de faire des recherches et de visualiser en temps réel sur l'écran iPhone la route à suivre vers n'importe quel commerce et la distance qui reste à parcourir. La « réalité augmentée » est une technologie de pointe intégrée aux applications qui font simultanément appel à la boussole 3GS, au GPS et à la caméra vidéo de l'iPhone. Comme le mentionne un communiqué de presse, « l'application de Canpages permet à l'utilisateur de chercher une certaine catégorie de commerces —

> les utilisateurs peuvent naviguer "virtuellement" dans les rues pour voir si un restaurant offre du stationnement ou pour jeter un coup d'œil à la vitrine d'un magasin en particulier[21].

Le lancement de Scène de rues a eu lieu en mars 2009 et permettait de voir Vancouver, Squamish et Whistler en ligne[22]. En août 2009, Canpages a tourné des images des rues du centre-ville et des artères commerciales de Toronto[23] et de Montréal[24], et ces deux villes sont maintenant visibles en ligne.

2. Politique de confidentialité

La politique de confidentialité de Canpages[25] donne les précisions suivantes concernant l'outil Scène de rues :

> Dans son effort de fournir le Service Vue de la rue (Street Scene) [habituellement appelé Scène de rues] de Canpages, Canpages fait preuve de sensibilité pour éviter d'inclure des informations de nature photographique qui fourniraient de l'information personnelle au sujet de personnes identifiables. Nous sommes sensibles à l'égard des préoccupations relatives à la confidentialité que pourraient avoir certaines personnes ayant été photographiées lors de la préparation des données requises par le service Vue de la rue (Street Scene). Les photographies de personnes identifiables ne sont aucunement requises par le service. L'assemblage des données est conçu de manière à flouter consciemment les visages de toute personne pouvant être photographiée dans le cadre de cette démarche. Vous constaterez, par conséquent, que personne ne peut être identifié en utilisant le service Mapjack. Si vous souhaitez faire part d'une préoccupation concernant la confidentialité, veuillez cliquer sur « Faire part d'une préoccupation » sur l'une des pages du Service Vue de la rue.

La politique de confidentialité précise également ceci : « Nos politiques de confidentialité reposent sur les 10 principes d'équité dans le traitement des renseignements personnels tels que décrits par le Commissaire à la protection de la vie privée du Canada ». Les dix principes sont ensuite énumérés.

---

21 Canpages inc., « Canpages to Begin Street Scene Shooting in Toronto », 11 août 2010, http://corporate.canpages.ca/media/Street%20Scene%20Toronto%20Shoot.pdf.

22 Kris Abel, « Canada AM—Street View Comes to Canada With New Tricks From CanPages.ca », CTV.ca, blogue de Kris Abel, 16 mars 2009, http://krisabel.ctv.ca/post/Canada-AM-e28093-Street-View-Comes-To-Canada-With-New-Tricks-From-CanPagesca.aspx.

23 Canpages inc., « Canpages to Begin Street Scene Shooting in Toronto », 11 août 2009, http://corporate.canpages.ca/media/Street%20Scene%20Toronto%20Shoot.pdf, et Kenyon Wallace, « Google Street View gets Canpages competition », *Toronto Star*, 11 août 2009, http://www.thestar.com/business/companies/google/article/679194--google-street-view-gets-canpages-competition.

24 Roberto Rocha, « Canpages Street Scene launches in Montreal », *Montreal Gazette*, 27 août 2009, http://www.canada.com/montrealgazette/Canpages+Street+Scene+launches+Montreal/1938073/story.html.

25 Accessible en ligne : http://www.canpages.ca/hm/privacy.jsp?lang=1.

recommandations formulées ci-dessus ont été mises en œuvre; elle produira à ce moment-là son rapport final avec ses conclusions[18].

Dans un article paru le 22 octobre 2010, le journaliste Michael Liedtke de l'*Associated Press* a signalé que Google « serre la vis à ses employés pour qu'ils n'empiètent pas sur la vie privée des gens pendant la collecte et le stockage de renseignements[19] ». Selon lui, « en plus de nommer une employée de longue date, Alma Whitten, directrice de la protection de la vie privée, Google a dit vendredi qu'elle obligera ses 23 000 employés à suivre une formation. La société est aussi en train d'implanter de nouvelles mesures de vérification pour que les travailleurs obéissent aux règles. L'adoption de mesures plus strictes semble faire suite aux manquements récents qui ont soulevé des doutes sur les contrôles et les politiques internes ». Lorsqu'il a témoigné devant le Comité le 4 novembre 2010, le conseiller en matière de politique au Canada de Google, Jacob Glick, a confirmé que son entreprise était en train de prendre ces mesures.

D. Scène de rues de Canpages

1. Le service

Canpages, une entreprise canadienne offrant un annuaire en ligne pour les recherches d'entreprises, a lancé, en partenariat avec une société américaine appelée MapJack, un service qui fera concurrence à l'outil Street View de Google[20]. Tout comme l'outil Street View de Google Maps, le service Scène de rues de Canpages offre des images panoramiques des voies urbaines, ce qui permet aux utilisateurs d'explorer des quartiers entiers en quelques clics de souris. Toutefois, contrairement au service Street View de Google, le service Scène de rues de Canpages se concentre sur les commerces. Ainsi, comme l'indique un communiqué de presse :

> Scène de rues fournit des vues panoramiques de 360 degrés des voies urbaines aux utilisateurs effectuant des recherches d'entreprises locales sur Canpages.ca. Cette technologie leur permet de cibler les résultats de recherche sur une carte géographique et d'en obtenir des images à haute résolution dans l'environnement local. Par exemple,

---

18 Ibid.

19 Michael Liedtke, « Google to impose tougher privacy measures after backlash to recent employee missteps, breaches », *Canadian Business Online*, 22 octobre 2010, http://www.canadianbusiness.com/markets/headline_news/article.jsp?content=b4915117&page=2.

20 Kris Abel, « Canada AM—Street View Comes to Canada With New Tricks From CanPages.ca », CTV.ca, blogue de Kris Abel, 16 mars 2009, http://krisabel.ctv.ca/post/Canada-AM-e28093-Street-View-Comes-To-Canada-With-New-Tricks-From-CanPagesca.aspx. Canpages est la plus importante entreprise locale de recherches locales et le plus grand éditeur d'annuaires au Canada. Son site Web, Canpages.ca, offre des bases de données résidentielles et commerciales nationales et plus de 3,5 millions de visiteurs uniques visitent le site chaque mois pour y effectuer des demandes de recherches locales. Forte de 80 publications et comptant plus de 80 000 clients, Canpages rejoint plus de huit millions de foyers et d'entreprises d'un bout à l'autre du Canada. Le siège social est situé à Vancouver, et quelque 700 personnes sont à l'emploi de Canpages dans ses bureaux de l'Alberta, de la Colombie-Britannique, de l'Ontario et du Québec : http://corporate.canpages.ca/about_us/company_profile/where_local_search_gets_done.

Le 31 mai 2010, après avoir appris que des véhicules Street View avaient recueilli des données utiles transmises sur des réseaux Wi-Fi non cryptés pendant la collecte de signaux radio Wi-Fi diffusés publiquement, le Commissariat à la protection de la vie privée du Canada a déposé trois plaintes contre Google conformément au paragraphe 11(2) de la LPRPDE[15].

Les trois plaintes sont les suivantes :

a. Google aurait recueilli, utilisé ou communiqué des données utiles sans avis et consentement préalable;

b. Google aurait recueilli des données utiles sans déterminer les fins de la collecte de renseignements personnels au préalable;

c. Google aurait recueilli des données utiles au-delà de ce qui est nécessaire aux fins déterminées[16].

Au terme de son enquête, la commissaire à la protection de la vie privée a, le 19 octobre 2010, publié une *Lettre de conclusions préliminaire*[17] (annexe B), où elle recommandait que Google instaure un modèle de gouvernance permettant de respecter les lois canadiennes sur la protection de la vie privée. Le modèle comprendrait des mesures de contrôle qui feraient en sorte que les procédures nécessaires au respect de la vie privée aient été suivies avant le lancement d'un produit.

La commissaire a aussi recommandé que Google améliore la formation offerte à tous ses employés au sujet du respect de la vie privée et désigne une ou des personnes responsables de la protection de la vie privée et du respect des obligations de leur entreprise à cet égard, ce qui est une exigence des lois canadiennes en la matière.

Elle a recommandé en outre que Google supprime les données utiles recueillies au Canada, dans la mesure où les lois canadiennes et américaines ne l'empêchent pas de le faire, ce qui pourrait être le cas par exemple pour préserver des éléments de preuve dans le cadre de poursuites judiciaires. Si les données utiles canadiennes ne pouvaient pas être supprimées sur-le-champ, il faudrait les conserver de manière sécuritaire et en restreindre l'accès .

La commissaire à la protection de la vie privée ne considérera l'affaire comme résolue que si Google lui remet au plus tard le 1er février 2011 la confirmation que les

---

15 Paragraphe 11(2) de la LPRPDE : « Le commissaire peut lui-même prendre l'initiative d'une plainte s'il a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question relative à l'application de la présente partie. »

16 Commissariat à la protection de la vie privée du Canada, *Lettre de conclusions préliminaire*, 19 octobre 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_f.cfm.

17 *Ibid.*

Comment signaler un problème

Si vous avez trouvé une image Street View que vous considérez comme inappropriée, procédez comme suit :

1. Localisez l'image dans Street View.
2. Cliquez sur « Signaler un problème » dans l'angle situé en bas à gauche de l'image.
3. Remplissez le formulaire, puis cliquez sur « Envoyer ».

C'est tout. Nous examinerons votre rapport très rapidement[12].

3. Collecte, par Google, de données utiles dans des réseaux Wi-Fi non protégés et conclusions préliminaires du Commissariat à la protection de la vie privée

Après que l'organisme allemand de protection des renseignements personnels situé à Hambourg lui eut demandé de vérifier les données Wi-Fi recueillies par ses véhicules Street View dans le cadre d'un projet de services géodépendants, Google a découvert en mai 2010 qu'elle avait recueilli des données utiles (le contenu de communications faites dans un réseau) transmises sur des réseaux sans fil non protégés pendant sa collecte de renseignements sur les points d'accès Wi-Fi à l'appui d'un projet de services géodépendants. Un service géodépendant est un service d'information et de divertissement accessible au moyen d'un appareil mobile dans le réseau mobile et qui tire parti de la capacité d'utiliser la position géographique de l'appareil[13]. De l'aveu même de Google, cette collecte accidentelle semble avoir été causée par l'intégration d'un code au logiciel élaboré pour capter les signaux Wi-Fi. Devant cette situation, la société a immobilisé ses véhicules Street View, arrêté de recueillir des données sur les réseaux Wi-Fi le 7 mai 2010 et isolé et stocké toutes les données déjà recueillies[14].

---

12 http://maps.google.ca/help/maps/streetview/privacy.html.

13 « Location-Based Services », GSM Association, janvier 2003, http://www.gsmworld.com/documents/se23.pdf.

14 Commissariat à la protection de la vie privée du Canada, *Lettre de conclusions préliminaire*, 19 octobre 2010, http://www.priv.gc.ca/media/nr-c/2010/let_101019_f.cfm.

photos pour Street View. De plus, la société Google devra publier trois jours à l'avance sur son site Web les noms des zones qu'elle entend photographier et communiquer la même information dans au moins une station radio et deux journaux locaux pour que les résidants puissent avoir le choix d'éviter de se faire photographier. Google sera passible d'amendes pouvant aller jusqu'à 180 000 euros pour avoir enfreint le nouveau règlement italien[11].

2. Protection de la vie privée

Google, sur son site Web, fournit aux utilisateurs les renseignements suivants concernant la protection de la vie privée :

> **Accès public uniquement**
>
> La fonctionnalité Street View propose des photographies tout à fait semblables à ce que vous voyez lorsque vous vous promenez dans la rue, que ce soit en voiture ou à pied. Ces images sont aujourd'hui disponibles pour de nombreuses villes du monde. Dans certains cas, Google prévoit de conclure des partenariats, à l'instar de celui réalisé avec Disneyland Paris, pour planifier la prise de photos des lieux.
>
> **Les images Street View ne sont pas en temps réel**
>
> Nos images affichent uniquement ce que nos véhicules ont pu voir le jour lorsqu'ils sont passés dans un lieu précis. Ensuite, plusieurs mois sont nécessaires pour traiter les images recueillies avant de les mettre en ligne. Les images que vous voyez dans Street View peuvent donc être datées de quelques mois à quelques années.
>
> **Les personnes et les plaques d'immatriculation sont rendues floues**
>
> Nous avons mis au point une technologie très sophistiquée permettant de rendre flous des visages et des plaques d'immatriculation. Elle est utilisée dans toutes les images Street View. Par conséquent, si un visage reconnaissable (par exemple, celui d'un passant sur le trottoir) ou une plaque d'immatriculation lisible figure sur l'une de nos photos, [cette portion d'image] est automatiquement rendue floue par notre technologie, afin que la personne ou le véhicule en question ne puisse pas être identifié. Si nos détecteurs ont laissé passer quelque chose, n'hésitez pas à nous le faire savoir.
>
> **Vous pouvez demander le retrait d'une image**
>
> Nous offrons des outils faciles d'accès afin de permettre à tout utilisateur de demander le retrait d'une image dont il juge le contenu inapproprié (en cas de nudité, par exemple) ou sur laquelle il se reconnaît lui-même, sa famille, sa voiture ou son domicile. La procédure permettant d'effectuer ce type de demande est décrite ci-dessous.

---

11 « Italy privacy regulator orders restrictions on Google's Street View », *International Business Times*, 26 octobre 2010, http://www.ibtimes.com/articles/75777/20101026/google-street-view-italy.htm.

L'application Street View peut maintenant être consultée pour la plupart des régions peuplées du Canada, comme le montre la carte du site Web de Google, http://www.google.com/intl/fr_us/help/maps/streetview/where-is-street-view.html, qui indique les régions du monde répertoriées. Ce site donne aussi un aperçu des zones où les véhicules de Google sont actuellement en activité.

Tout au long de 2009, la commissaire à la protection de la vie privée du Canada a mené des discussions avec Google inc. pour informer l'entreprise des dispositions législatives protégeant la vie privée au Canada et elle a fait part de ses inquiétudes concernant la surveillance caméra nécessaire pour offrir le service Street View. À la suite de consultations avec la commissaire, la société Google a accepté de brouiller les visages et les plaques d'immatriculation dans les images canadiennes du service Street View.

Le service de Google couvre déjà la majeure partie des États-Unis et a été lancé dans plus de 100 villes à l'échelle du monde. Il a généré une controverse considérable. Par exemple, en mai 2009, l'Agence de protection des données en Grèce a interdit à Google de prendre des photos Street View à Athènes, exigeant plus de garanties de la part de la société en matière de protection de la vie privée, comme des avis publics annonçant quand les véhicules de tournage circulent et l'amélioration de la protection des images stockées[8]. Au Japon, les plaintes de la population ont forcé Google à baisser ses caméras de 40 centimètres afin que les images soient prises au niveau des yeux et non par-dessus les clôtures, dans les cours intérieures[9].

En février 2010, les organismes de réglementation de la protection des renseignements personnels de l'Union européenne ont demandé à Google d'informer la population avant d'envoyer des caméras dans les villes pour son service Street View. Ils ont aussi écrit à Google pour lui demander de raccourcir la durée de conservation des photos originales pour la ramener d'un an à six mois. Dans une déclaration tenant lieu de réponse, Google a affirmé que son besoin de conserver les images Street View pendant un an est légitime et justifié[10].

En octobre 2010, l'organisme de protection de la vie privée de l'Italie a annoncé que des restrictions étaient imposées au service de cartographie de Street View, faisant ainsi écho aux préoccupations exprimées ailleurs en Europe. Il a précisé dans une déclaration que, dorénavant, les véhicules de Google devront être « clairement identifiés par des pancartes et des auto-collants » indiquant qu'ils sont en train de prendre des

---

8 Derek Gatopoulos, « Google's Street View halted in Greece over privacy », *USA Today*, 12 mai 2009, http://www.usatoday.com/tech/news/2009-05-12-google-street-view_N.htm. « Google Street View faces privacy roadblocks in Japan, Greece », CBC News Online, 13 mai 2009, http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html.

9 « Google Street View faces privacy roadblocks in Japan, Greece », CBC News Online, 13 mai 2009, http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html.

10 Aoife White, « Google warned by EU over Street View map photos », *The Globe and Mail*, 26 février 2010, http://www.theglobeandmail.com/news/technology/google-warned-by-eu-over-street-view-map-photos/article1482311/.

Les entreprises qui offrent ces applications d'imagerie doivent également avoir une bonne raison pour conserver les images originales et non brouillées dans leurs bases de données. Si elles conservent des images non brouillées, elles doivent cependant limiter la période durant laquelle elles les gardent et les protéger avec des mesures de sécurité appropriées[3].

C. Street View de Google

1. Le service

Le service Street View est créé par Google inc., une entreprise offrant un moteur de recherche sur le Web, et offert dans le cadre de Google Maps. Il reproduit la vue de la rue qu'un utilisateur aurait s'il se promenait dans un lieu géographique donné quelque part dans le monde. L'utilisateur n'a qu'à cliquer sur une carte du service à http://Maps.google.ca/streetview, et faire une *promenade virtuelle* dans le quartier choisi, reconstruit en ligne au moyen d'images photographiques des environs.

Ces photographies sont prises par des photographes qui se déplacent dans des villes et d'autres sites cartographiés à bord de voitures identifiées surmontées de caméras. Les photographes ont commencé à visiter les villes canadiennes et à prendre des photos en 2007, mais ces images ont été entreposées pour usage futur[4]. Le lancement officiel des activités de cartographie photographique de Google au Canada a eu lieu en mars 2009, dans 11 villes canadiennes[5], et le service lui-même a été lancé au Canada en octobre 2009. Les visites par les Canadiens sur le site ont plus que doublé après le lancement[6].

La société Google a annoncé le 22 mars 2010 qu'elle passerait plusieurs mois à photographier les rues des villes, grandes et petites, de l'ensemble des provinces et des territoires du Canada. Quand tout sera terminé, le Canada, comme les États-Unis, le Royaume-Uni et la France, aura accès à un service Street View à l'échelle du pays. La société a également affirmé qu'elle retournerait à Windsor pour reprendre des photographies de la ville, car des conseillers municipaux se sont plaints des photos existantes, qui ont été réalisées au cours de la longue grève des travailleurs municipaux l'été précédent. Les photos prises au printemps montrent des rues négligées et des monceaux de déchets à de nombreux endroits[7].

---

3 *Ibid.*

4 CBC News, « Google Alerts Canadians About Street View Filming », CBC News Online, 26 mars 2009, http://www.cbc.ca/technology/story/2009/03/26/tech-090326-google-street-view.html.

5 « Google Street View faces privacy roadblocks in Japan, Greece », CBC News Online, 13 mai 2009, http://www.cbc.ca/world/story/2009/05/13/google-street-view-japan-greece.html.

6 Vito Pilieci, « Canadian Street View snoopers pump up Google's hits; Privacy concerns remain as more than 28 million images viewed in one day », *Ottawa Citizen*, 10 octobre 2009.

7 CBC News, « Google Street View to expand in Canada », CBC News, 22 mars 2010, http://www.cbc.ca/technology/story/2010/03/22/google-street-view-windsor-canada.html.

soulève des préoccupations nouvelles qui touchent la nécessité pour les concepteurs de technologies comme Google de prendre des mesures pour bien protéger la vie privée des citoyens dans l'élaboration de nouveaux produits.

B. La protection des renseignements personnels au Canada

La collecte, l'usage et la communication de renseignements personnels par les entreprises au Canada sont régis par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cependant, dans les provinces qui ont adopté leur propre loi « essentiellement similaire » à la loi fédérale, les organismes régis par la loi provinciale sont soustraits à l'application de la loi fédérale. Ainsi, en Colombie-Britannique, ce genre d'activité est régi par la *Personal Information Protection Act*, en Alberta par la *Personal Information Protection Act*, et au Québec par la *Loi sur la protection des renseignements personnels dans le secteur privé*[1].

En avril 2009, la commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, a envoyé au Comité une lettre accompagnée d'une fiche d'information produite par son bureau et intitulée « Vous êtes photographié — La technologie de l'imagerie à l'échelle de la rue, Internet et vous[2] » (annexe A). La fiche d'information fait part de certaines préoccupations en matière de protection de la vie privée soulevées par la commissaire et ses homologues provinciaux en ce qui concerne les applications de l'imagerie à l'échelle de la rue :

> Les commissaires à la protection de la vie privée ont tenu des discussions avec diverses entreprises pour renforcer les mécanismes de protection des personnes dont la photo a été prise. Nous croyons que toutes les entreprises qui offrent de telles applications doivent prendre des mesures pour mieux protéger votre vie privée.
>
> En plus de demander aux entreprises d'être plus proactives et originales dans leurs communications avec le public pour veiller à ce que les Canadiennes et les Canadiens soient informés du moment où leurs villes — et par conséquent eux-mêmes — pourraient être photographiées, nous croyons qu'elles devraient adopter une attitude plus sensible au respect de la vie privée lorsqu'elles choisissent les endroits à photographier. Les personnes qui pénètrent dans des lieux, comme des refuges ou des cliniques d'avortement, où la confidentialité est d'une importance capitale ou qui en sortent veulent vraisemblablement conserver l'anonymat pour des raisons liées à leur vie privée ou à leur sécurité.
>
> Les entreprises devraient également utiliser des technologies de brouillage efficaces et éprouvées des visages et des numéros de plaques d'immatriculation de façon à ce que les personnes ne puissent être identifiées lorsque leurs photos sont affichées sur Internet. Dans ces cas, les entreprises devraient offrir des mécanismes rapides et réactifs qui permettent de bloquer ou de retirer les images.

---

1 En Ontario, la situation est quelque peu différente : dans cette province, la plupart des renseignements personnels détenus par des entreprises sont régis par la LPRPDE, mais les renseignements personnels liés à la santé relèvent d'une loi provinciale, soit la *Loi sur la protection des renseignements personnels sur la santé*.

2 Disponible aussi en ligne : http://www.priv.gc.ca/fs-fi/02_05_d_39_prov_f.cfm.

LA PROTECTION DE LA VIE PRIVÉE DANS LE MONDE NUMÉRIQUE : ÉTUDE DES RÉPERCUSSIONS SUR LA VIE PRIVÉE DES SYSTÈMES D'IMAGERIE À L'ÉCHELLE DE LA RUE

CONTEXTE

A. L'étude du Comité

Le 27 avril 2009, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ci-après le Comité) a adopté la motion suivante :

> Que, le comité étudie les répercussions qu'ont sur la vie privée les systèmes de caméras de surveillance comme les applications « Street View » de Google et Canpages et d'autres questions liées à la surveillance vidéo et que le comité demande à Eric Schmidt, président-directeur général de Google, ou à une personne le représentant au Canada, et à Olivier Vincent, président-directeur général de Canpages, ou à une personne le représentant, de témoigner à ce sujet devant ses membres.

L'étude du Comité a porté sur la technologie de l'imagerie à l'échelle de la rue, qui a recours à divers moyens pour photographier les paysages de rue. Généralement, on utilise une caméra montée sur un véhicule qui sillonne les rues des villes choisies. Les images peuvent ensuite être visionnées sur Internet.

Le Comité a recueilli les témoignages de Jonathan Lister, directeur général et chef de Google Canada, et d'Olivier Vincent, président-directeur général de Canpages, le 17 juin 2009, ainsi que d'Elizabeth Denham, commissaire adjointe fédérale à la protection de la vie privée, le 22 octobre 2009.

On a découvert en mai 2010 que des véhicules Street View de Google avaient recueilli des données utiles à partir de réseaux sans fil non protégés pendant leur collecte de données Wi-Fi. Au terme de l'enquête faite ultérieurement par le Commissariat à la protection de la vie privée sur les manquements aux règles de protection de la vie privée qu'a pu entraîner la collecte de données Wi-Fi, le Comité a entendu le témoignage du Commissariat le 28 octobre 2010 et celui de Jacob Glick, conseiller en matière de politique au Canada chez Google, le 4 novembre 2010. Le 25 novembre 2010, le Comité a de nouveau entendu M. Glick, ainsi que la nouvelle directrice de la protection de la vie privée chez Google, Alma Whitten, par téléconférence, de même que François D. Ramsay, premier vice-président, conseiller juridique principal, secrétaire et responsable du respect de la vie privée et Martin Aubut, premier directeur, Commerce social, tous deux du Groupe Pages jaunes (Canpages).

Bien que l'étude du Comité ait pour thème les répercussions des systèmes d'imagerie à l'échelle de la rue sur la vie privée, le cas des données Wi-Fi de Google

TABLE DES MATIÈRES

LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l'honneur de présenter son

ONZIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(3)*h*)(vi) du Règlement, le Comité a étudié la question des répercussions sur la vie privée des systèmes d'imagerie à l'échelle de la rue et a convenu de faire rapport de ce qui suit :

LA PROTECTION DE LA VIE PRIVÉE DANS LE MONDE NUMÉRIQUE : ÉTUDE DES RÉPERCUSSIONS SUR LA VIE PRIVÉE DES SYSTÈMES D'IMAGERIE À L'ÉCHELLE DE LA RUE

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président

L' hon. Shawn Murphy, C.P., député

JANVIER 2011

40e LÉGISLATURE, 3e SESSION

Publié en conformité de l'autorité du Président de la Chambre des communes

On peut obtenir des copies supplémentaires en écrivant à :
Les Éditions et Services de dépôt Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à
l'adresse suivante : http://www.parl.gc.ca

CHAMBRE DES COMMUNES
CANADA

LA PROTECTION DE LA VIE PRIVÉE DANS LE MONDE NUMÉRIQUE : ÉTUDE DES RÉPERCUSSIONS SUR LA VIE PRIVÉE DES SYSTÈMES D'IMAGERIE À L'ÉCHELLE DE LA RUE

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président

L' hon. Shawn Murphy, C.P., député

JANVIER 2011

40e LÉGISLATURE, 3e SESSION